54Mbps Wireless Broadband Router

WRT-414

User's Manual

Copyright

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

To assure continued compliance.(example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm(8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

WEEE regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User's Manual for PLANET 54Mbps Wireless Broadband Router

Model: WRT-414

Rev: 1.0 (August. 2005)

Part No. EM-WRT414

TABLE OF CONTENTS

Chapter 1 Introduction

Thank you for purchasing WRT-414. This manual guides you on how to install and properly use the WRT-414 in order to take full advantage of its features.

1.1 Package Contents

Make sure that you have the following items:

- One WRT-414
- One AC Power Adapter
- One User's Manual CD
- One Quick Installation Guide
- One External Dipole Antenna

Note:	If any of the above items are missing, contact your supplier for support.

1. 2 Features

- Compliant with 802.11g / 802.11b standard
- Allow multiple users to share a single Internet connection
- Internet Access via Cable or xDSL modem
- Access Private LAN Servers from the Public Network
- AP / AP Client / WDS / Bridge modes supported
- Equipped with four LAN ports (10/100M) and one WAN port (10/100M), Auto-MDI/MDI-X supported
- Support DHCP Server for easy setup
- System status monitoring including Active DHCP Client, Security Log and Device/Connection Status
- Easy to use Web-based GUI for configuration and management purposes
- Remote Management allows configuration and upgrades from a remote site (over the Internet)
- DHCP/PPPoE/PPTP/L2TP/Fixed IP allocation
- MAC/IP filter access control, URL blocking
- SPI firewall + DoS prevention protection
- Support UPnP function
- Supports 64/128-bit WEP, WPA-PSK, WPA, WPA2 Encryption to protect the wireless data transmissions

1.4 Specification

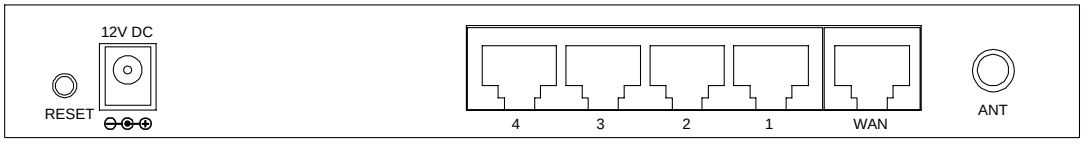
Standard	IEEE 802.11g/802.11b Compliant
Signal Type	DSSS (Direct Sequence Spread Spectrum)
Modulation	OFDM/ QPSK / BPSK / CCK

WAN Port	1 x 10/100Base-TX, Auto-MDI/MDI-X
LAN Port	4 x 10/100Base-TX, Auto-MDI/MDI-X
Antenna	Dipole Antenna * 1
Data Encryption	64 bit / 128 bit WEP, WPA-PSK, WPA, WPA2
Frequency	2.4GHz - 2.484GHz
Sensitivity	**11g @ PER < 10%** 54Mbps: -71.46 dBm 48Mbps: -73.1 dBm 36Mbps: -75 dBm 24Mbps: -77 dBm 18Mbps: -79.1 dBm 12Mbps: -81.1 dBm 9Mbps: -83.5 dBm 6Mbps: -85.52 dBm **11b @ PER < 8%** 11Mbps: -82 dBm 5.5Mbps: -85.7dBm 2Mbps: -87 dBm 1Mbps: -91.5 dBm
Data Rate	Up to 54Mbps (with automatic scale back)
LED Indicators	PWR, WLAN LAN: LNK/ACT * 4, 10/100Mbps * 4 WAN: LNK/ACT * 1, 10/100Mbps * 1
Power Requirement	12V DC, 1A
Power Consumption	TX power consumption: <650mA RX power consumption <350mA
Temperature	Operating :0 ~ 55 degree C Storage: -20 ~ 70 degree C
Humidity	Operating: 0 ~ 90% Storage: 0 ~ 95% Non-Condensing
Dimensions	190 x 98 x 35 mm
Output Power	18dBm

Chapter 2 Hardware Installation

Before you proceed with the installation, it is necessary that you have enough information about the WRT-414.

2.1 Hardware Connection



1. **Locate an optimum location for the WRT-414.** The best place for your WRT-414 is usually at the center of your wireless network, with line of sight to all of your mobile stations.
2. **Adjust the antennas of WRT-414.** Try to adjust them to a position that can best cover your wireless network. The antenna's position will enhance the receiving sensitivity.
3. **Connect RJ-45 cable to WRT-414 LAN port.** Connect one of the LAN ports on WRT-414 to your LAN switch/hub or a computer with a RJ-45 cable.
4. **Connect RJ-45 cable to WRT-414 WAN port.** Connect xDSL/Cable Modem to the WAN port on WRT-414. Usually, this cable would be provided with your modem. If no cable was supplied with your modem, please use a RJ-45 Ethernet cable
5. **Plug in power adapter and connect to power source**. After power on, WRT-414 will start to operate.

Note: ONLY use the power adapter supplied with the WRT-414. Otherwise, the product may be damaged.
If you want to reset WRT-414 to default settings, press and hold the Reset button over 5 seconds and release. And then wait for WRT-414 restart.

Reset Button	This button has two functions: **To Reboot machine without Clearing Existing Configurations:** Press the reset button with a pencil tip (for less than 5 seconds), machine will re-boot itself, the existing configurations will be kept. **To Clear All Data and restore the factory default values:** Press the reset button for longer than 5 seconds and the router will reset itself to the factory default settings (warning: your original configurations will be replaced with the factory default settings)

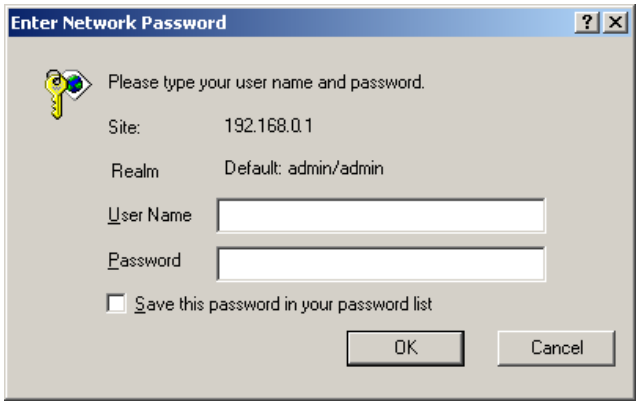
2.2 LED Indicators

LED		Color	STATE	MEANING
PWR		Green	On	Device power on
			Off	Device power off
			Blinking	During boot up procedure.
WLAN		Orange	Blinking	Transmitting or receiving data through the Wireless LAN
			Off	Wireless LAN is no function
WAN	**10/100M**	Green	On	WAN port is connected at 100Mbps
			Off	WAN port is connected at 10Mbps
	LNK/ACT	Green	On	Link is established
			Blinking	Packets are transmitting or receiving
LAN	**10/100M**	Green	On	LAN is connected to 100Mbps device
			Off	LAN is connected to 10Mbps device
	LNK/ACT	Green	On	Link is established
			Blinking	Packets are transmitting or receiving
			Off	LAN port is not connected

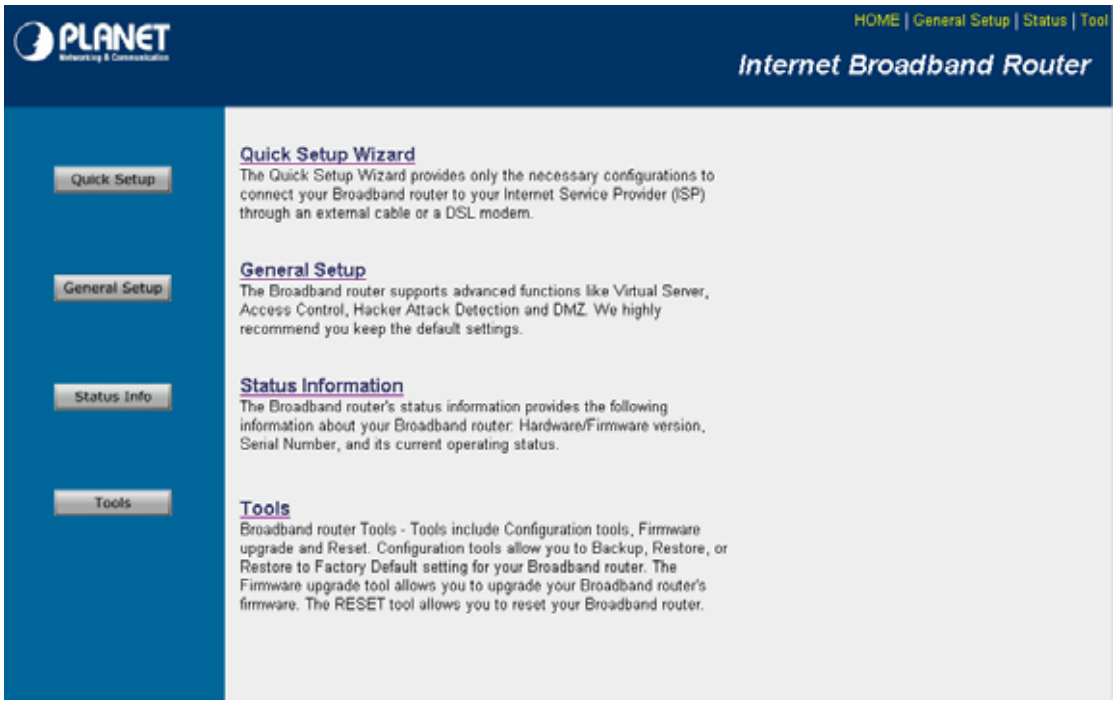
Chapter 3 Web Login

Web configuration provides a user-friendly graphical user interface (web pages) to manage your WRT-414. A WRT-414 with an assigned IP address will allows you to monitor and configure via web browser (e.g., MS Internet Explorer or Netscape).

1. Open your web browser.
2. Enter the IP address of your WRT-414 in the address field (default IP address is http://192.168.0.1).
3. A User Name and Password dialog box will appear. Please enter your User Name and Password here. Default User Name and Password are both “admin”. Click OK.



4. Then you will see the WRT-414 main page as below.



The left panel provides four options, **Quick Setup**, **General Setup**, **Status Information** and **Tools**.

Section	Description
Quick Setup	Select your Internet connection type and then input the configurations needed

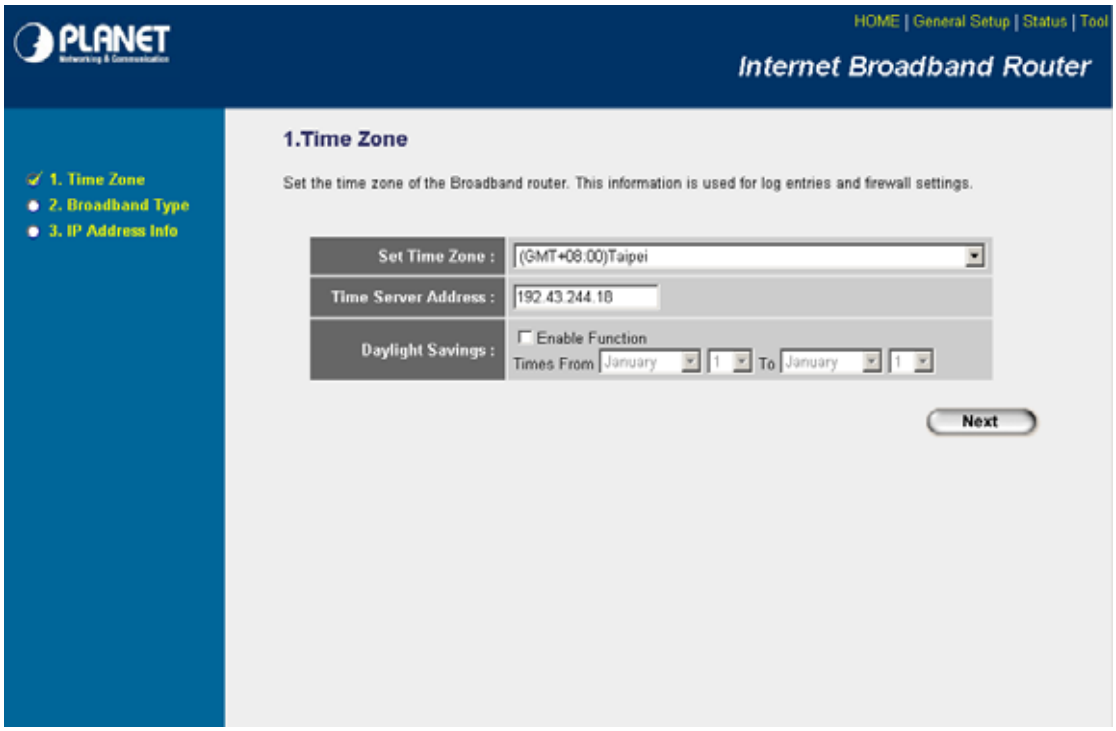
	to connect to your Internet Service Provider (ISP).
General Setup	This section contains configurations for the Broadband router's advance functions such as: Port Forwarding, Virtual Server, Access Control, Hacker Attack Prevention, DMZ, Special applications and other functions to meet your LAN requirements. You can also configure the wireless detail settings here.
Status Information	This option provides you the system information, Internet Connection, Device Status, Security Log and DHCP client Log information.
Tools	This option contains Configuration tools, Firmware Upgrade and Reset functions.

Chapter 4 Quick Setup

This section describes the basic configuration of the WRT-414 and allows you to connect to Internet easily.

4.1 Time Zone

The time information is used for Log entries and Firewall settings. You can keep the default Time Server address or set a new IP address for your router to synchronize its time. Click “Next” to continue.

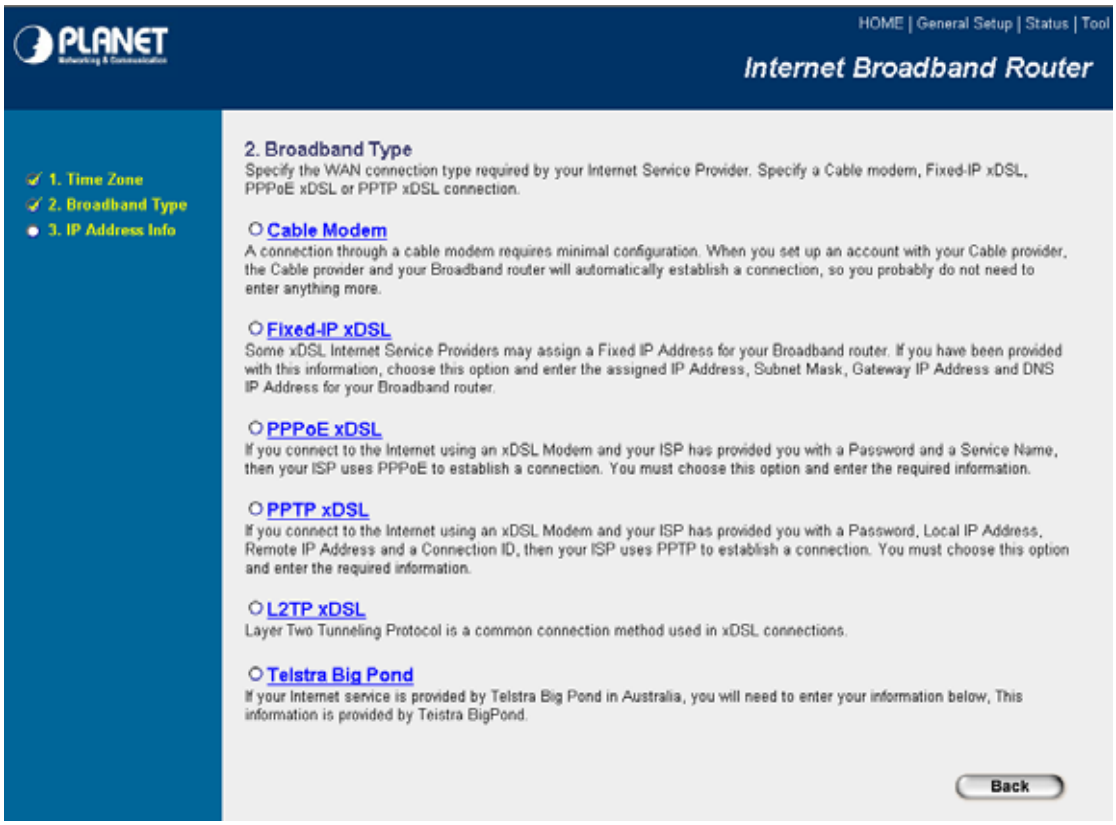


Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Time Server Address	Remain it as default or, you can manually assign an IP address of the Time Server. The information of Timer Server can be found in the following URL link: http://www.eecis.udel.edu/~mills/ntp/servers.html or http://www.ntp.org.
Enable Daylight Savings	The router can also take Daylight savings into account. To enable this function, check/tick the “Enable Function” box and select the which days this function will work .

Click “Next” button to proceed to the next step.

4.2 Broadband Type

Before establishing the Internet connection, please be sure to check with your ISP, and obtain all necessary information from them.

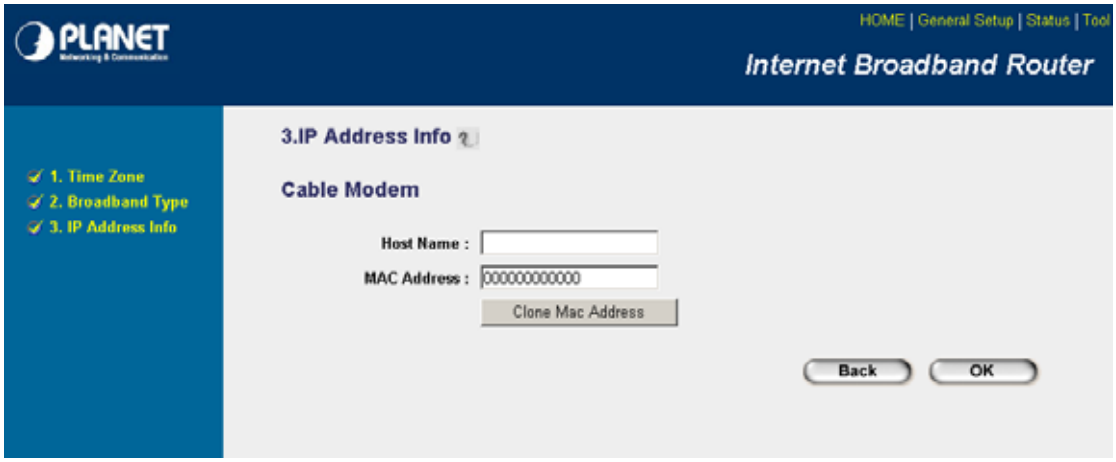


Broadband	Description
Cable Modem	ISP will automatically give you an IP address. Please refer to section 4.2.1 for details.
Fixed-IP xDSL	ISP has given you a fixed IP address already. Please refer to section 4.2.2 for details.
PPPoE xDSL	ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection. Please refer to section 4.2.3 for details.
PPTP xDSL	ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection. Please refer to section 4.2.4 for details.
L2TP XDSL	This is not widely used. You need to know the PPTP Server address as well as your name and password. Please refer to section 4.2.5 for details.
Telstra Big Pond	This option is for Australia only. Please refer to section 4.2.6 for details.

4.2.1 Cable Modem

With Cable Modem connection, the ISP will automatically give you an IP address. Some ISP may also require you to fill in additional information such as Host Name and MAC address (see screen below).

Note: The Host Name and MAC address section is **optional** and you can skip this section if your ISP does not require these settings for you to connect to the Internet.

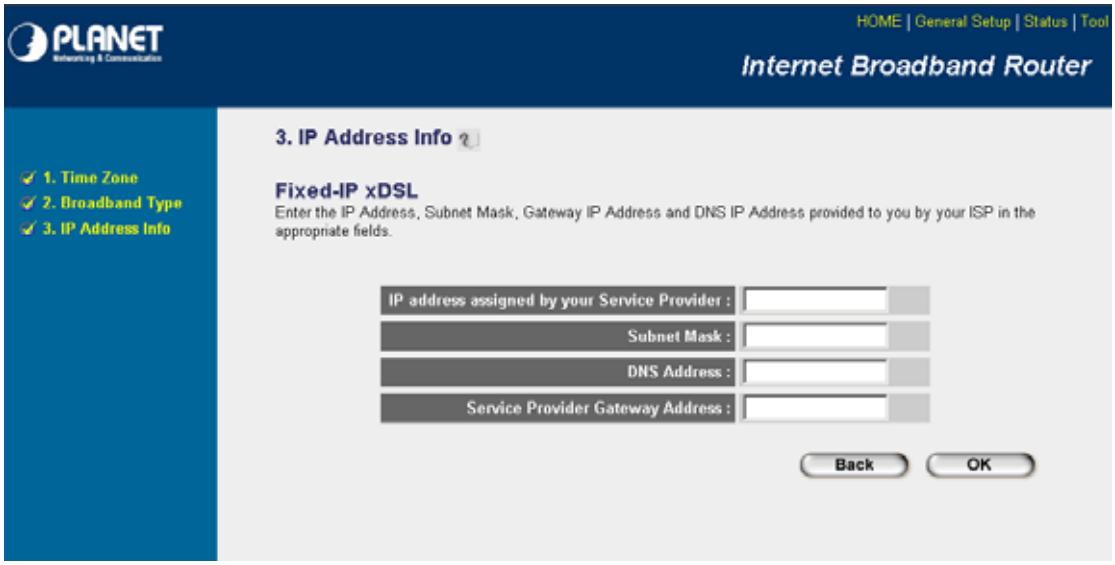


Parameters	Description
Host Name	Type in the host name provided by your ISP if any; otherwise, just leave it blank.
MAC Address	To connect to Internet, your ISP will require a MAC address from your PC. Type in this MAC address in this section or use the “Clone MAC Address” button to replace the WAN port MAC address with the your PC’s. To find out the PC’s MAC address, see Appendix A. (also see Glossary for an explanation on MAC address).

When the configuration finished, click “OK” to next step or click “Back” to previous step. After press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.2 Fixed-IP xDSL

Select Fixed-IP xDSL if your ISP has given you a specified IP address. Your ISP should provide all the information required in this section.



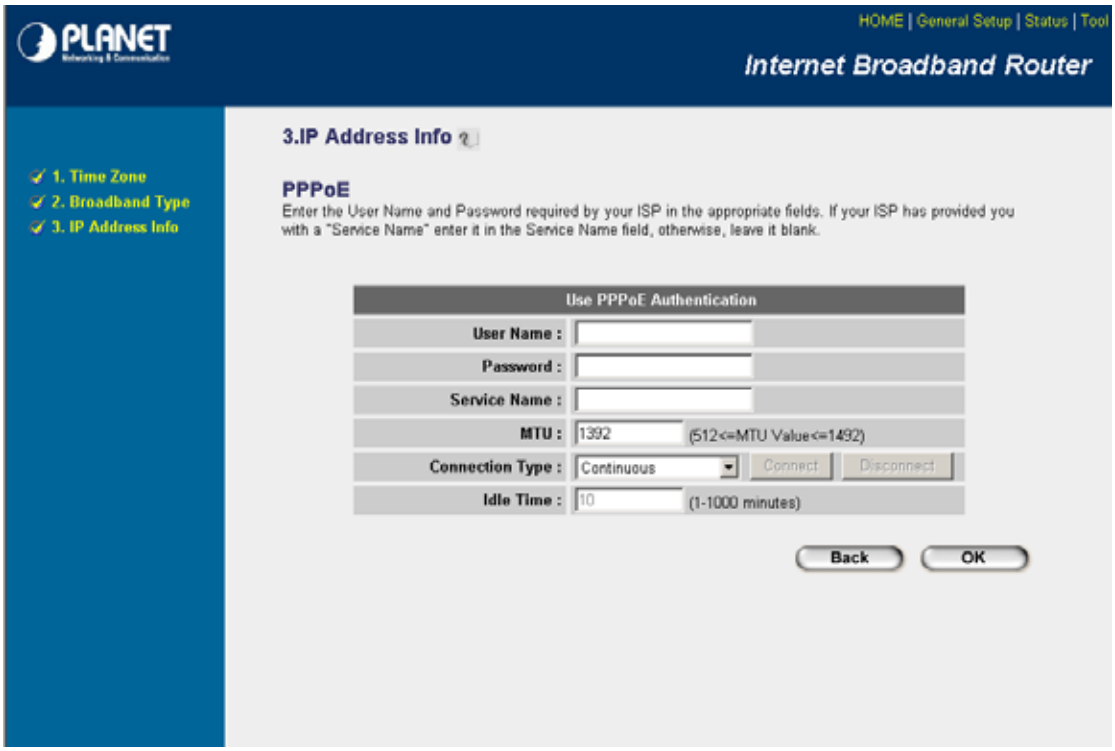
Parameters	Description
IP address assigned by your Service Provider	The IP address that your ISP should provide you.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0).
DNS Address	The IP address of ISP's DNS (Domain Name Service) Server.
Service Provider Gateway Address	The ISP's IP address gateway.

Please consult your local ISP about the information above.

When the configuration finished please click "OK" to next step or click "Back" to previous step. After press "OK", you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.3 PPPoE xDSL

Select PPPoE if your ISP requires the PPPoE protocol for Internet connectivity. Your ISP should provide all the information like user name, password required in this section.



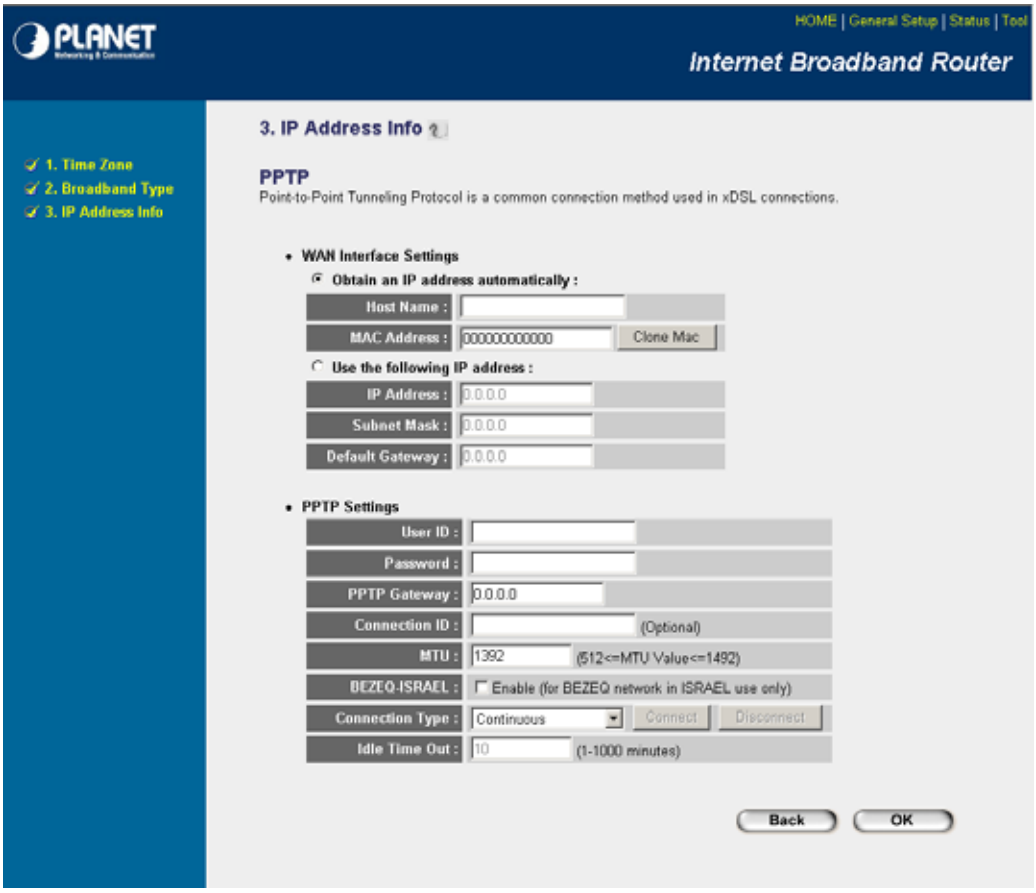
Parameters	Description
User Name	Enter the User Name provided by your ISP for the PPPoE connection.
Password	Enter the Password provided by your ISP for the PPPoE connection.
Service Name	This is an optional parameter. Leave it blank unless your ISP requires it.
MTU	This is an optional parameter. You can specify the maximum size of transmission packet to the Internet. The range of the MTU will be from 512 to 1492. You can also consult you ISP for the optimal MTU as well. Default: 1392.
Connection Type	If you select "**Continuous**", the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP. If you select "**Connect On Demand**", the router will auto-connect to the ISP when a client in LAN want to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "**Idle Time**". If you select "**Manual**", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP. Default: **Continuous**.
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no

	packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection from your ISP. **Note:** This “idle timeout” function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly, especially when your ISP charges you by time used.

When the configuration finished, click “OK” to next step or click “Back” to previous step. After press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.4 PPTP xDSL

Select PPTP if your ISP requires the PPTP protocol to connect to the Internet. Your ISP should provide all the information required in this section.



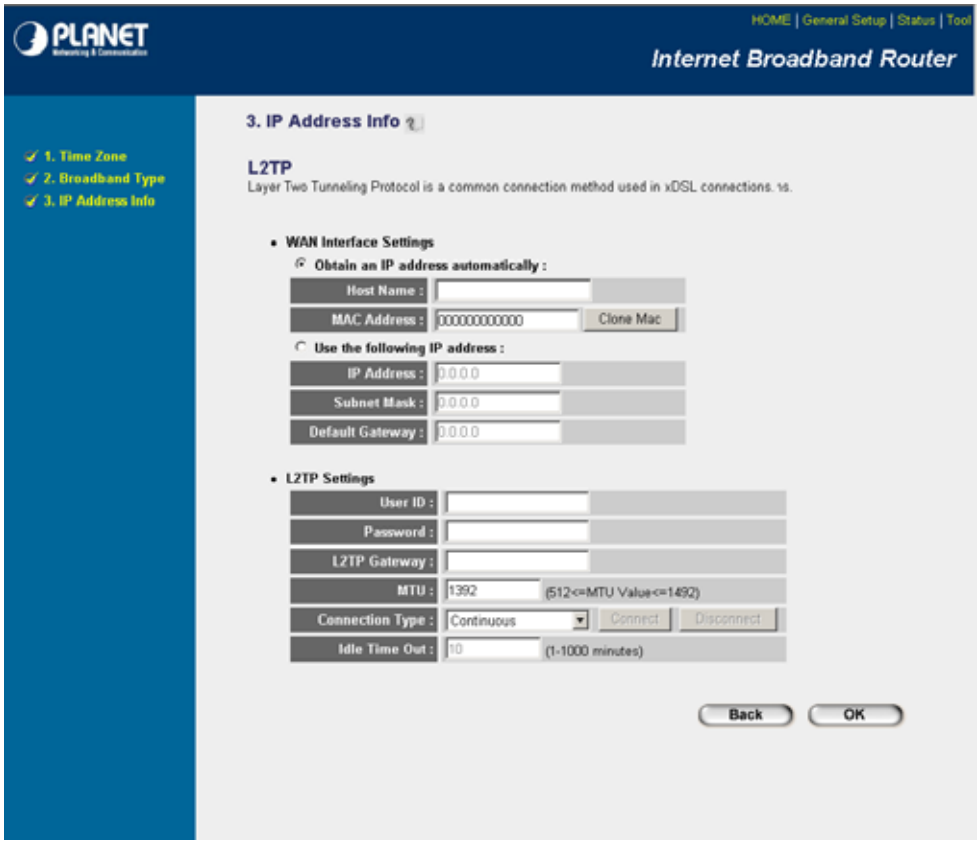
Parameter	Description
Obtain an IP address	Select it if the ISP requires you to obtain an IP address by DHCP automatically.
Host Name	Type in the host name provided by your ISP if any; otherwise, just leave it blank.
MAC Address	To connect to the Internet, your ISP will require a MAC address from your PC. Type in this MAC address in this section or use the “Clone MAC Address” button to replace the WAN port MAC address with the MAC address of that PC. To find out the PC’s MAC address, see Appendix A. (also see Glossary for an explanation on MAC address).
Use the following IP address	Select it if the ISP provides you a static IP to connect to the PPTP server.
IP Address	This is the IP address that your ISP has given you to establish a PPTP connection.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP’s Gateway.
User ID	Enter the User Name provided by your ISP for the PPTP connection. Sometimes called a Connection ID.
Password	Enter the Password provided by your ISP for the PPTP connection
PPTP Gateway	If your LAN has a PPTP gateway, enter that PPTP gateway’s IP address here. If you do not have a PPTP gateway, enter the ISP’s Gateway IP address above.
Connection ID	This is the ID given by ISP. This is an optional parameter.
MTU	This is an optional parameter. You can specify the maximum size of transmission packet to the Internet. The range of the MTU will be from 512 to 1492. You can also consult you ISP for the optimal MTU as well. Default: 1392
BEZEQ-ISRAEL	Select this item if you are using the service provided by BEZEQ in Israel.
Connection Type	If you select “**Continuous**”, the router will always connect to the ISP. If the WAN line breaks down and links again, the router shall auto- reconnect to the ISP. If you select “**Connect On Demand**”, the router will auto-connect to the ISP when a client in LAN wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the “Idle Time”. If you select “**Manual**”, the router will connect to ISP only when you click “Connect” manually from the Web user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP. Default: **Continuous.**
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) throughout this specified period, the router will automatically disconnect to with your ISP. **Note:** This “idle timeout” function may not work due to abnormal activities of

	some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly, especially when your ISP charges you by time used.

When the configuration finished please click “OK” to next step or click “Back” to previous step. After press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.5 L2TP xDSL

Select L2TP if your ISP requires the L2TP protocol to connect to the Internet. Your ISP should provide all the information required in this section.



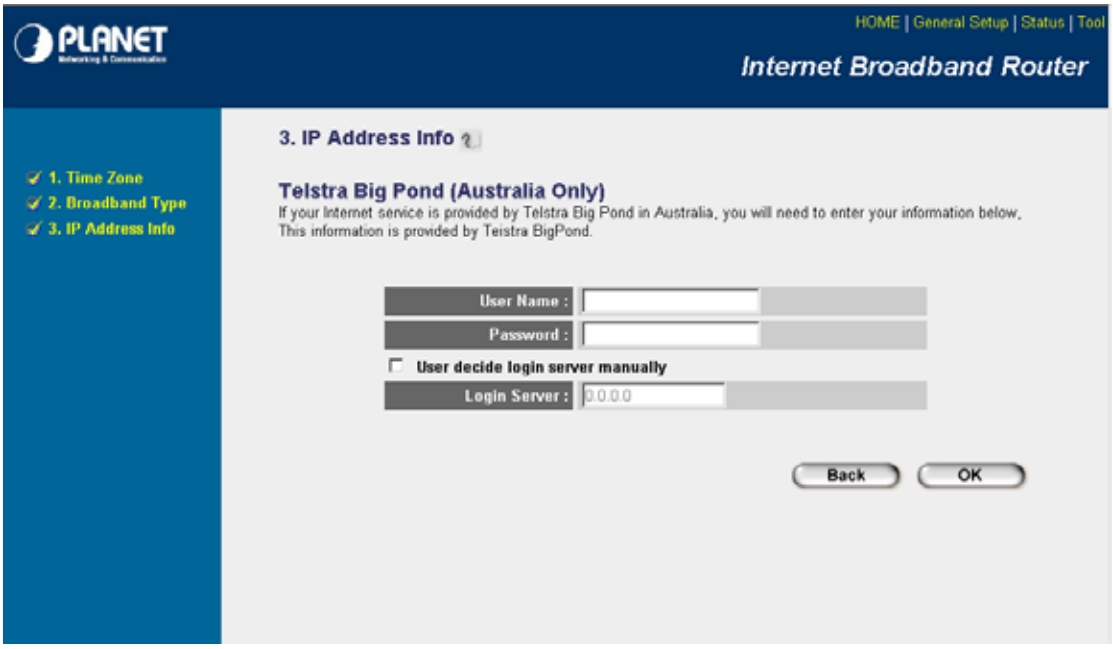
Parameter	Description
Obtain an IP address	Select it if the ISP requires you to obtain an IP address by DHCP automatically.
Host Name	If your ISP requires a Host Name, type in the host name provided by your ISP; otherwise, just leave it blank.
MAC Address	To connect to the Internet, your ISP will require a MAC address from your PC. Type in this MAC address in this section or use the “Clone MAC Address”

	button to replace the WAN port MAC address with the MAC address of that PC. To find out the PC's MAC address, see Appendix A. (also see Glossary for an explanation on MAC address.
Use the following IP address	Select it if the ISP provides you a static IP to connect to the L2TP server.
IP Address	This is the IP address that your ISP has given you to establish a L2TP connection.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP's Gateway.
User ID	Enter the User Name provided by your ISP for the L2TP connection. Sometimes called a Connection ID.
Password	Enter the Password provided by your ISP for the L2TP connection
L2TP Gateway	If your LAN has a L2TP gateway, enter that L2TP gateway's IP address here. If you do not have a L2TP gateway, enter the ISP's Gateway IP address above.
MTU	This is an optional parameter. You can specify the maximum size of transmission packet to the Internet. The range of the MTU will be from 1492 to 512. You can also consult you ISP for the optimal MTU as well. Default: 1392
Connection Type	If you select "**Continuous**", the router will always connect to the ISP. If the WAN line breaks down and links again, the router shall auto- reconnect to the ISP. If you select "**Connect On Demand**", the router will auto-connect to the ISP when someone want to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time". If you select "**Manual**", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP. Default: **Continuous.**
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) throughout this specified period, then the router will automatically disconnect the connection with your ISP. **Note:** This "idle timeout" function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly, especially when your ISP charges you by time used.

When the configuration finished please click “OK” to next step or click “Back” to previous step. After press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.6 Telstra Big Pond

Select Telstra Big Pond if you are live in Australia and your ISP requires this protocol to connect to the Internet. Your ISP should provide all the information required in this section.

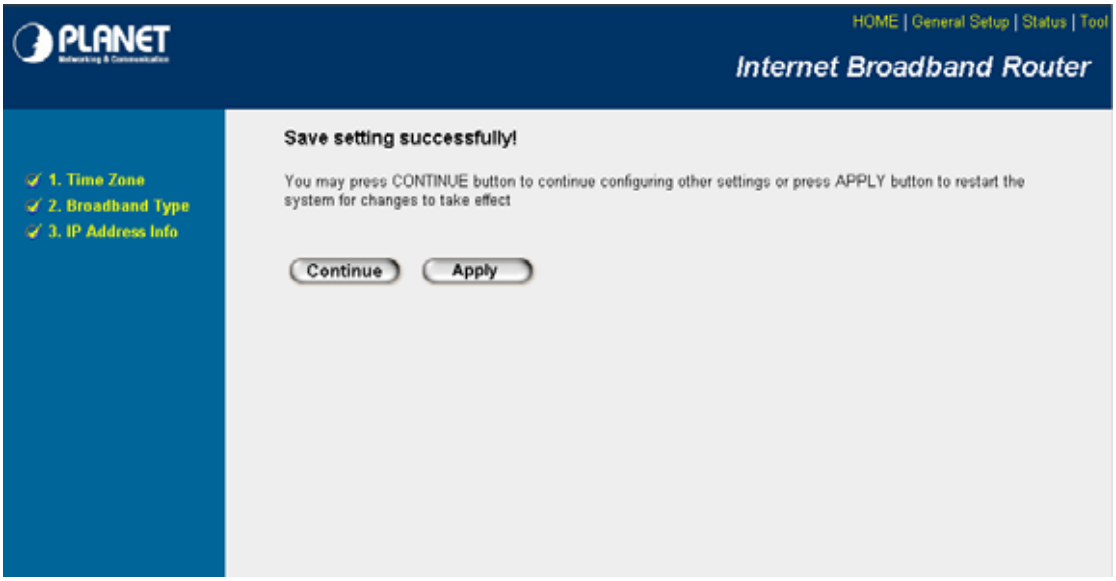


Parameters	Description
User Name	Enter the User Name provided by your ISP for the connection.
Password	Enter the Password provided by your ISP for the connection.
User Decide login server manually	If you ISP has provide the login server IP address to you, please check this box and enter the Login Server IP address below.
Login Server	Please enter the Login Server IP address here.

When the configuration finished please click “OK” to next step or click “Back” to previous step. After press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

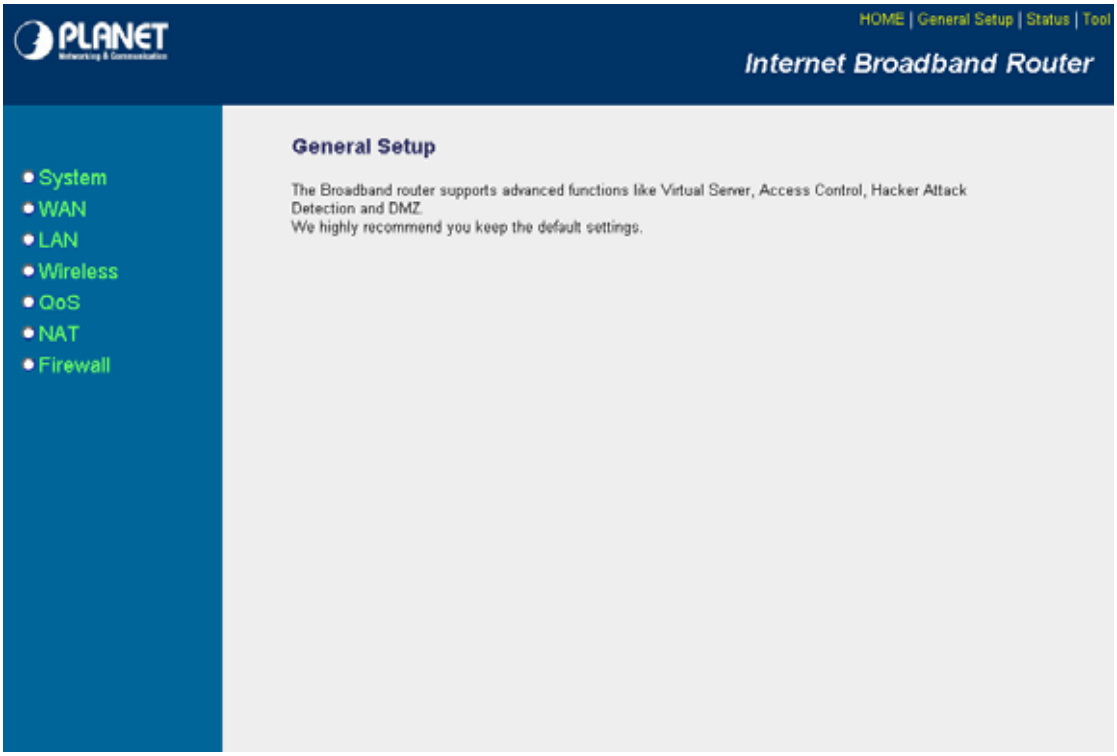
4.2.7 Save Settings Successfully

When you press “OK” in above configuration, the settings will be saved and the screen appears as below. Before WRT-414 restart, the settings are saved, but not function yet. You can also click “Continue” to configure other settings, this web page will appear when you save the settings in each configuration screen. Press “Apply” to restart the WRT-414 for the change to take effect immediately.


PLANET
HOME | General Setup | Status | Tool
Internet Broadband Router
1. Time Zone
2. Broadband Type
3. IP Address Info
Save setting successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Chapter 5 General Setup

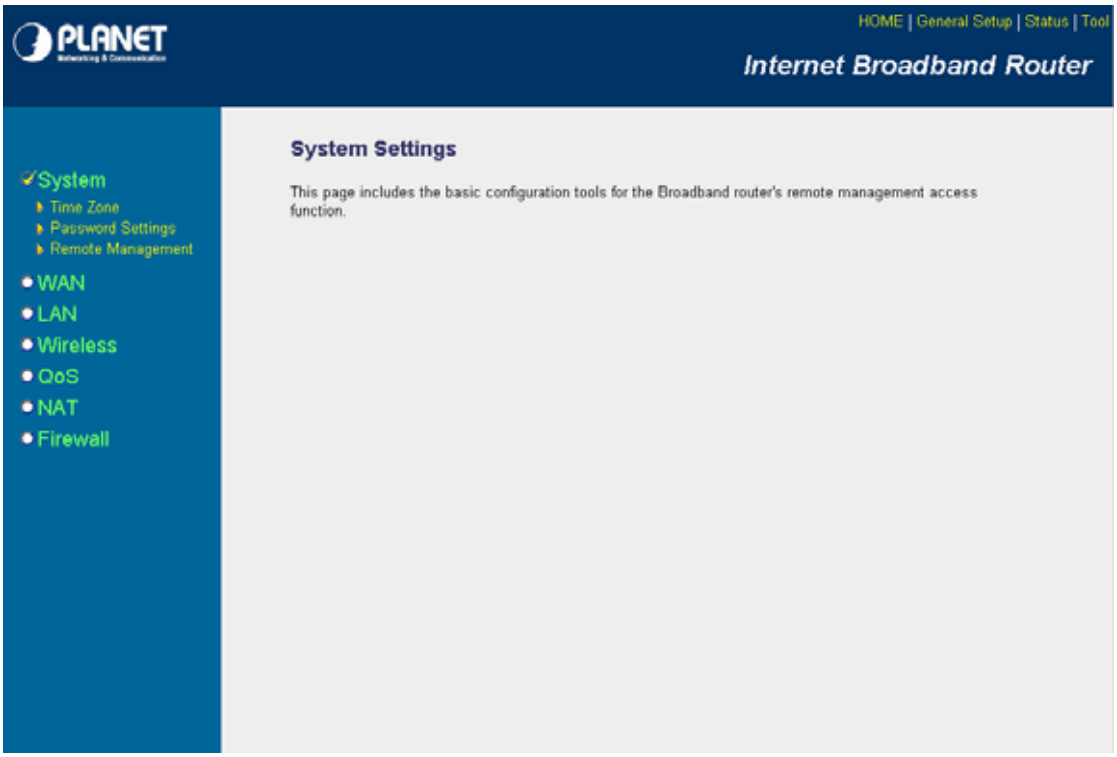
After click on the “General Setup” button at the main Page, you should see the screen below.



The General Setup contain advanced features that allow you to configure the router to meet the network’s needs such as: Wireless, Port Forwarding, Virtual Server, Access Control, URL Blocking, Special Applications, DMZ and other functions.

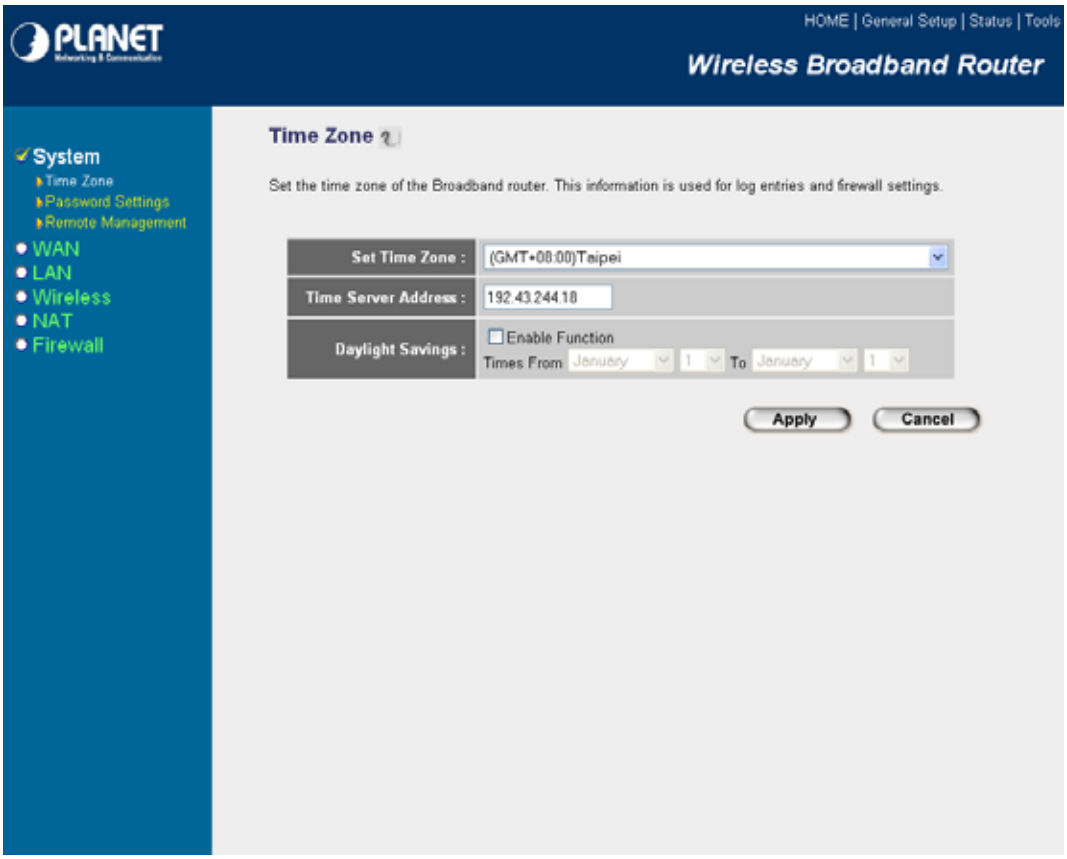
5.1 System

This section shows how to setup the Broadband router’s system Time Zone, Password and Remote Management Administrator.


PLANET
HOME | General Setup | Status | Tool
Internet Broadband Router
System
Time Zone
Password Settings
Remote Management
WAN
LAN
Wireless
QoS
NAT
Firewall
System Settings
This page includes the basic configuration tools for the Broadband router's remote management access function.

5.1.1 Time Zone

The Time Zone allows WRT-414 to allocate its time on the settings configured here, it will affect log display functions such as Security Log and Firewall settings.

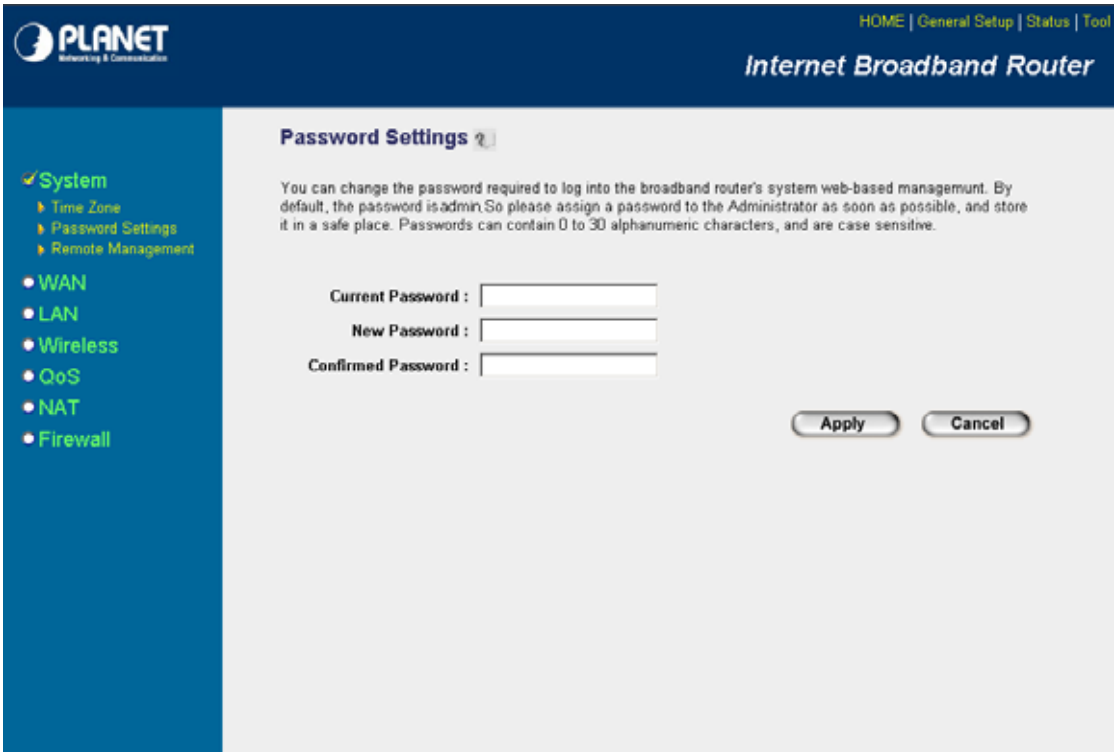


Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Time Server Address	You can keep the default IP address or enter a new Time Server Address for this device to synchronize its time. You can also refer to the web site http://www.ntp.org to find a nearest time server.
Daylight Savings	The router can also take Daylight savings into account. Select the check box to enable your daylight saving configuration. You can set the days that you wish to start and stop daylight Savings Time.

After the setup completed, please click “Apply” to save the settings. After press “Apply”, you will see a web screen to prompt you the configurations save successfully. You may refer to section 4.2.7 for the information of this screen.

5.1.2 Password Setup

This screen allows you to change the management password.



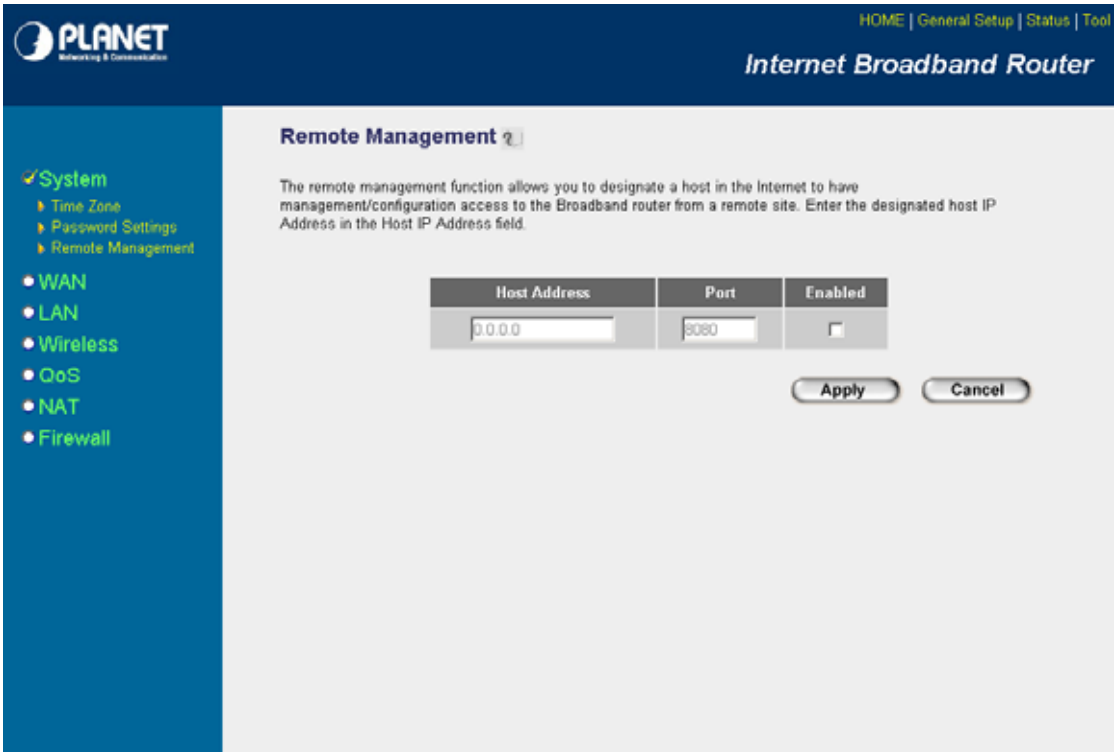
Parameters	Description
Current Password	Enter your current password for the remote management administrator to login to your Broadband router.
New Password	Enter your new password.
Confirmed Password	Enter your new password again for verification purposes.

After the setup completed, please click “Apply” to save the settings. After press “Apply”, you will see a web screen to prompt you the configurations save successfully. You may refer to section 4.2.7 for the information of this screen.

Note: If you forget the password, please reset the WRT-414 to the factory default by press reset button (on WRT-414’s rear panel) over 5 seconds.

5.1.3 Remote Management

You can specify a Host IP address that can perform remote management from Internet.



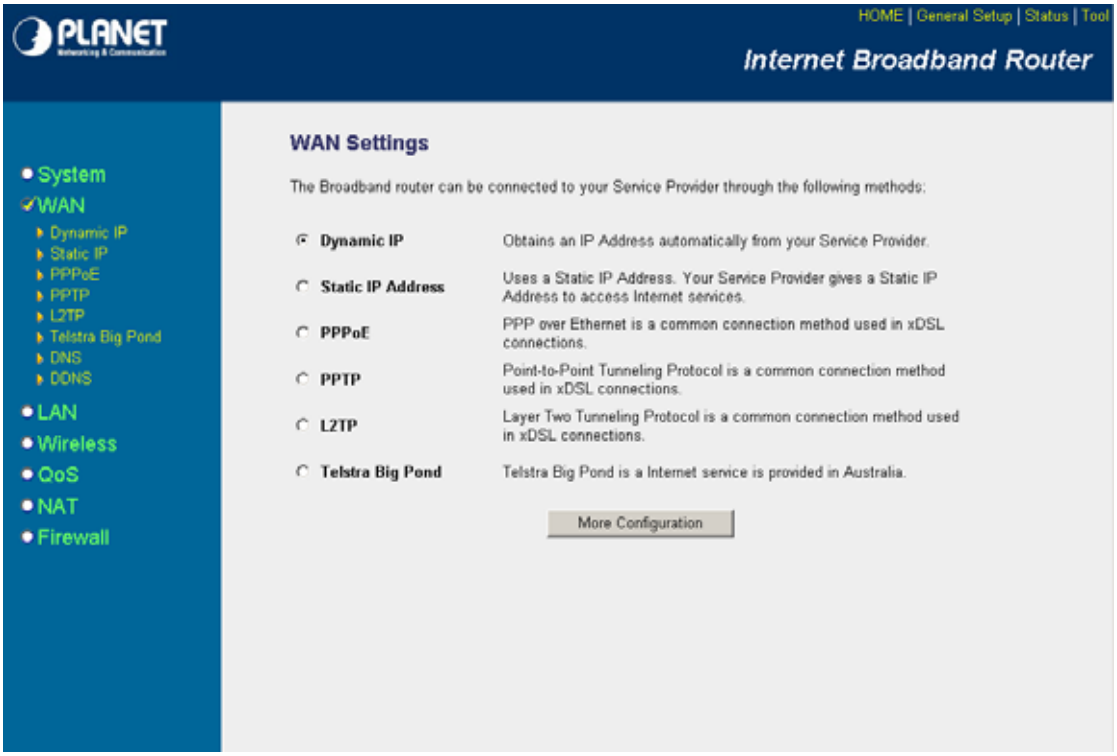
Parameters	Description
Host Address	The IP address of the host on Internet that will have management / configuration access to the Broadband router. Leave it to **0.0.0.0** means anyone can access the router's web-based configuration from any remote location. Click the **Enabled** box to enable the Remote Management function. **Note:** When you want to access the web-based management from a remote site, you must enter the router's WAN IP address (e.g. 10.0.0.1) into your web-browser followed by port number 8080, e.g. 10.0.0.1:8080 (see below). You'll also need to know the password set in the Password Setting screen in order to access the management pages.

After the setup completed, please click "Apply" to save the settings. After press "Apply", you will see a web screen to prompt you the configurations save successfully. You may refer to section 4.2.7 for the information of this screen.

5.2 WAN

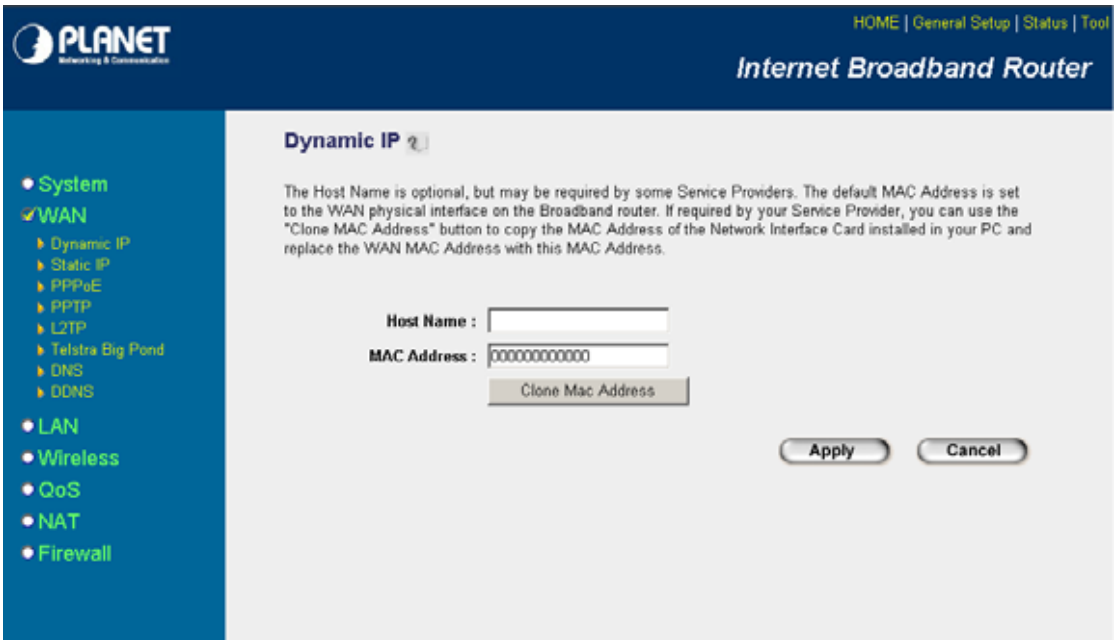
The WAN Settings screen allows you to specify the type of Internet connection. The WAN settings offer the following selections for the router's WAN port, **Dynamic IP**, **Static IP**, **PPPoE**, **PPTP**, **L2TP**, and

Telstra Big Pond. Please select one of the connection types and click “More Configuration” button or select the option on the left window for configurarion.



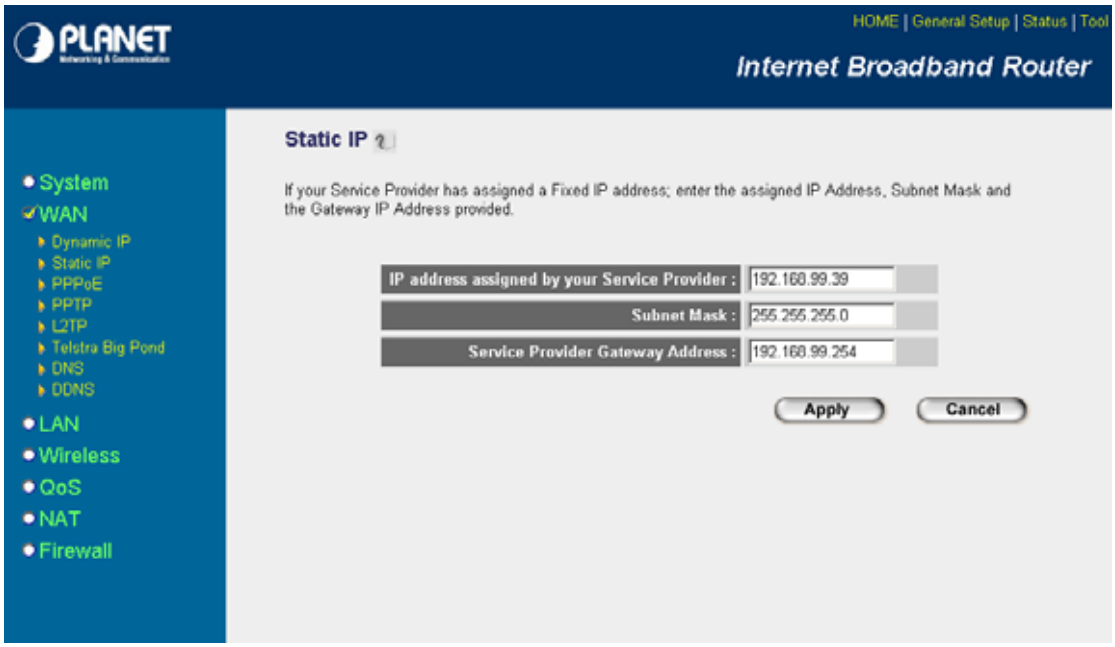
5.2.1 Dynamic IP

If Dynamic IP is selected, your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as Host Name, Domain Name and MAC address. Please refer to the section 4.2.1 for more settings of this option.



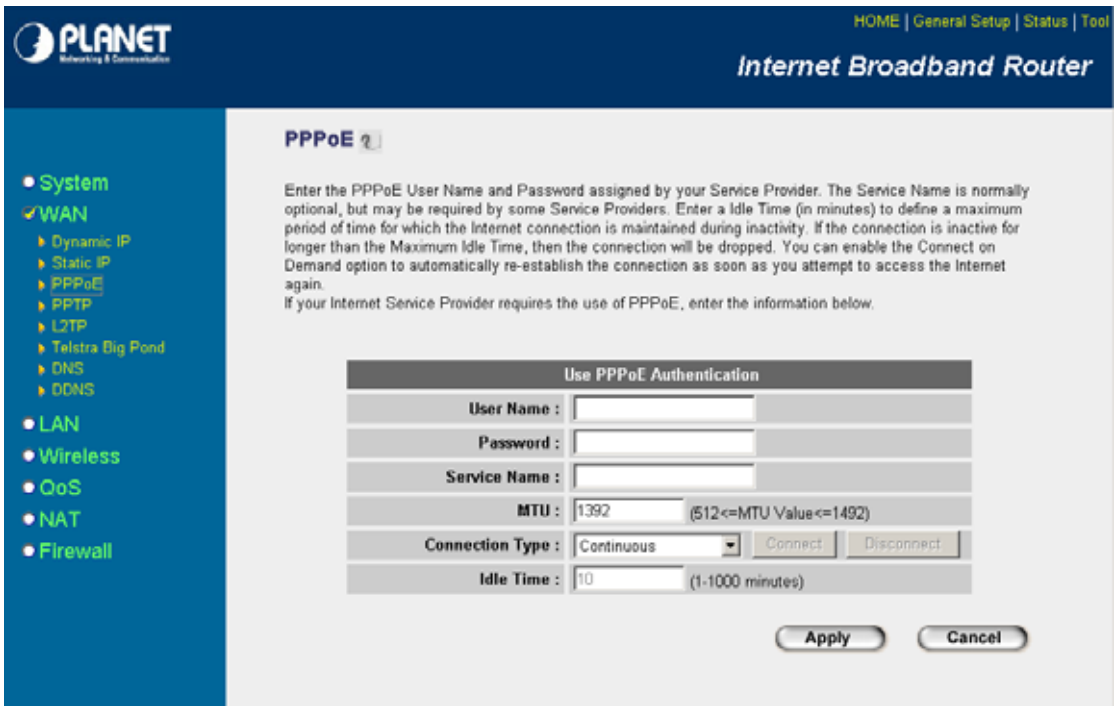
5.2.2 Static IP

If Static IP is selected, your ISP should provide all the information required in this screen. Please refer to the section 4.2.2 for more settings of this option.



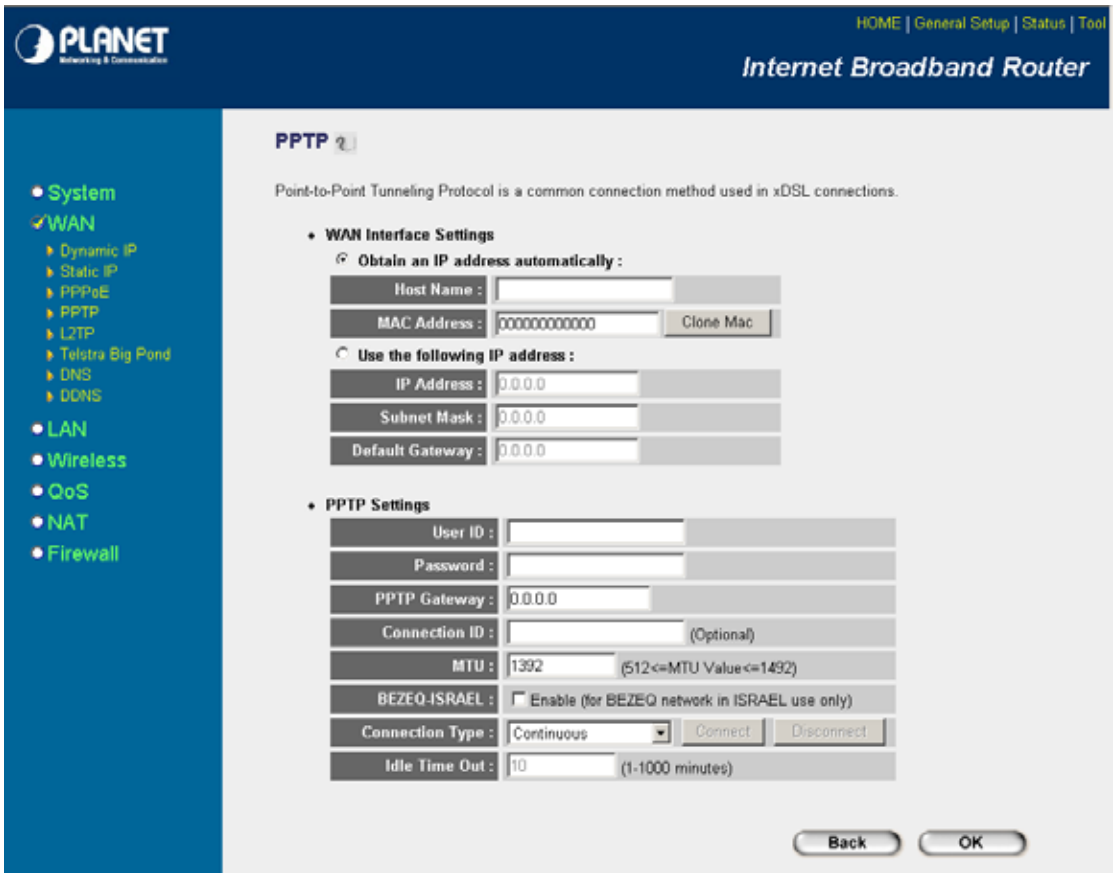
5.2.3 PPPoE

Select PPPoE if your ISP requires PPPoE protocol to connect to the Internet. Your ISP should provide all the information required in this section. Please refer to the section 4.2.3 to know the detail settings of this option.



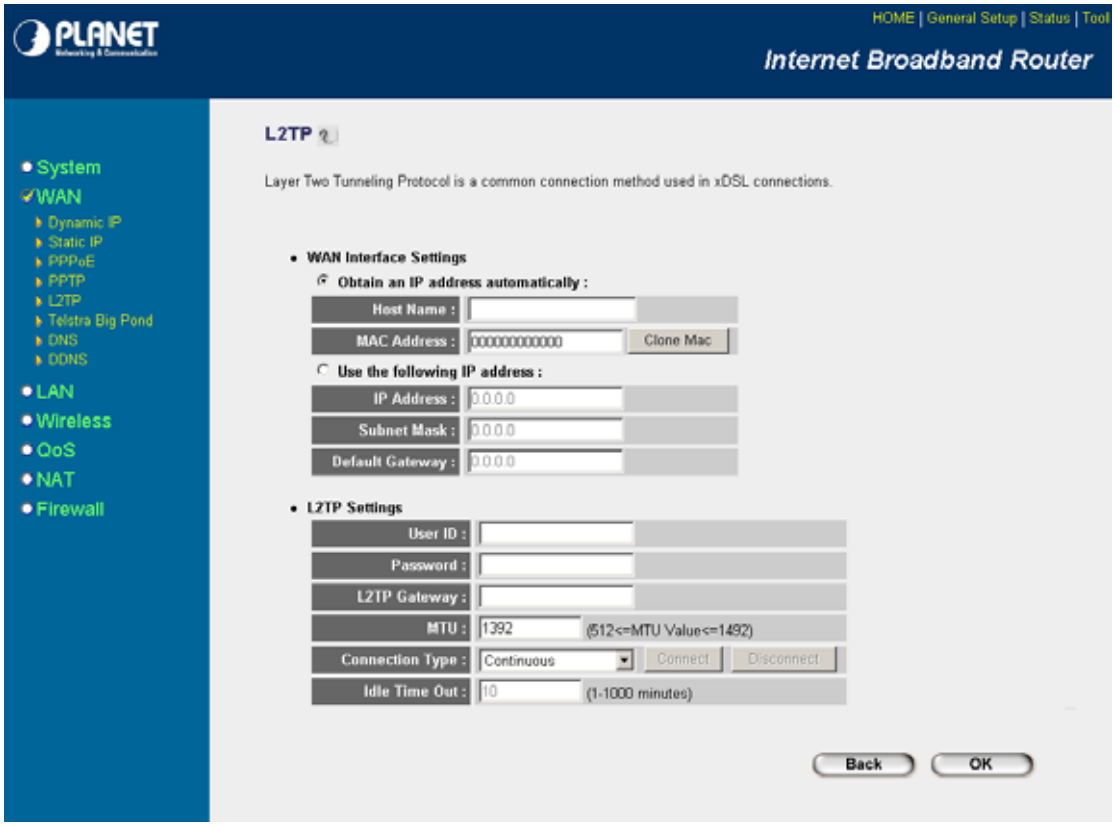
5.2.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect to the Internet. Your ISP should provide all the information required in this section. Please refer to section 4.2.4 for more settings of this option.



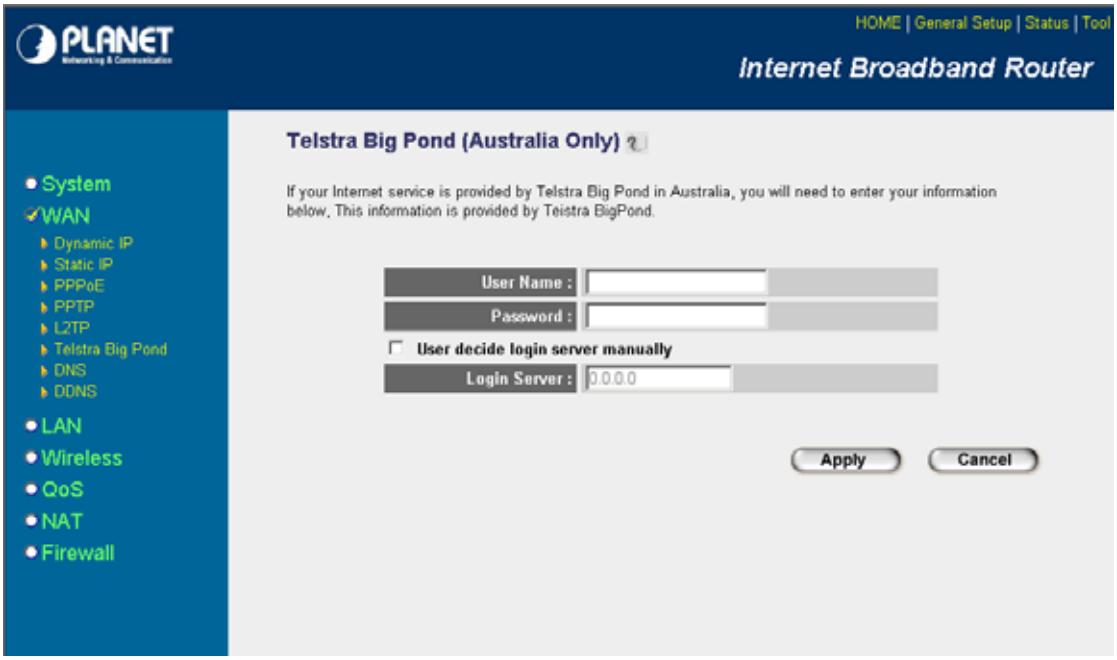
5.2.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect to the Internet. Your ISP should provide all the information required in this section. Please refer to section 4.2.5 for more settings of this option.



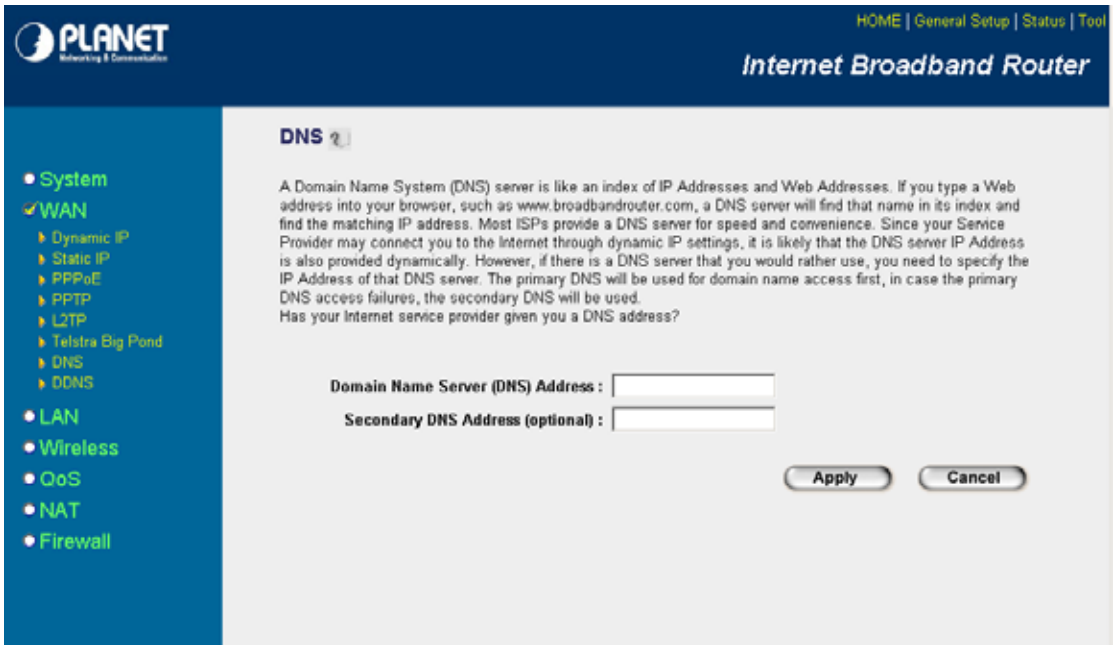
5.2.6 Telstra Big Pond

Select Telstra Big Pond if your ISP requires the Telstra Big Pond protocol to connect you to the Internet. Telstra Big Pond protocol is used by the ISP in Australia. Your ISP should provide all the information required in this section. Please refer to section 4.2.6 for more settings of this option.



5.2.7 DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.router.com, a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for efficiency and convenience. If your Service Provider connects you to the Internet with dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that you would rather to use, please specify the IP address of that DNS server here.

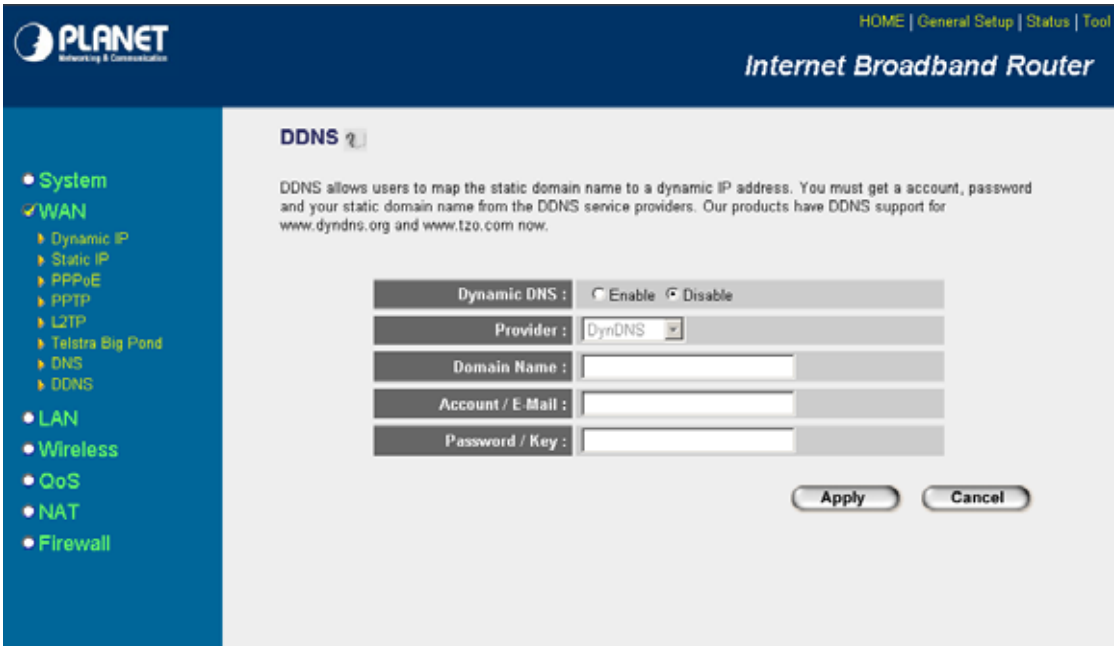


Parameters	Description
Domain Name Server (DNS) Server	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address.
Secondary DNS Address (optional)	This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used when the above primary DNS fails.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press "Continue" for configure other settings or "Apply" to restart WRT-414 with new configuration.

5.2.8 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS and TZO.

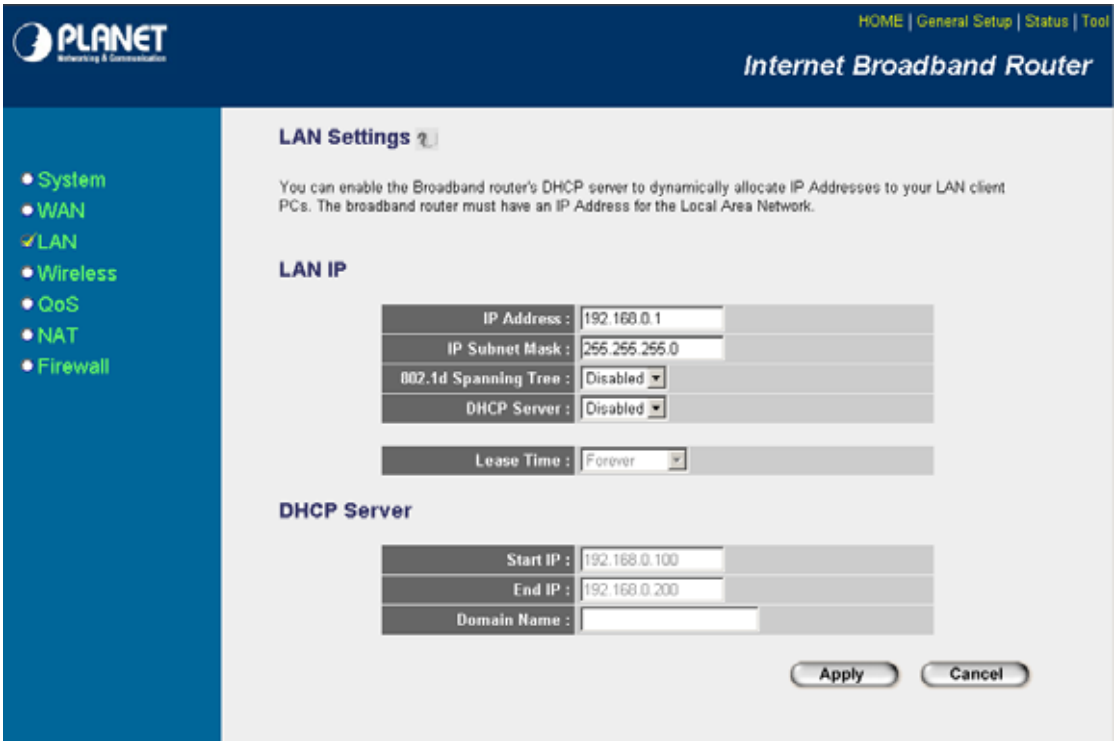


Parameters	Description
Dynamic DNS	Enable/Disable the DDNS function of this router.
Provider	Select a DDNS service provider. The default setting is “DynDNS”.
Domain name	Your static domain name that use DDNS.
Account / E-mail	The account that your DDNS service provider assigned to you.
Password / Key	The password you set for the DDNS service account above.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.3 LAN

The LAN Port screen below allows you to specify a private IP address for your router’s LAN interface.



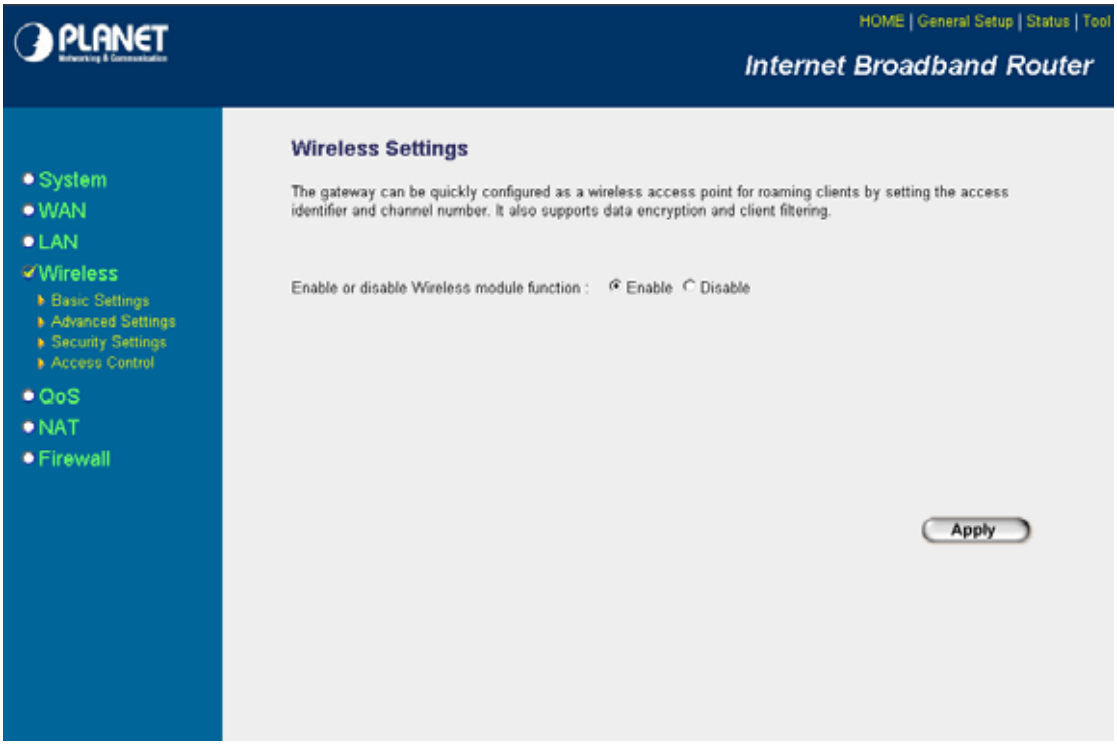
Parameters	**Description**
LAN IP	
IP Address	Designate the Access Point's IP Address. This IP Address should be unique in your network. The default IP Address is **192.168.0.1**.
Subnet Mask	Specify a Subnet Mask for your LAN segment. The Subnet Mask of the Access Point is fixed and the value is **255.255.255.0**.
802.1d Spanning Tree	If it is enabled, this router will use the spanning tree protocol to prevent from network loop happened in the LAN ports.
DHCP Server	Enable or disable the DHCP Server.
Lease Time	The DHCP Server will temporarily assign IP addresses to LAN clients. In the Lease Time setting you can specify the time period that the DHCP Server lends an IP address to your LAN client. The DHCP Server will change your LAN client's IP address when this time threshold period is reached.
IP Address Pool	
Start IP/End IP	You can designate a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. By default the IP range is from: Start IP **192.168.0.100** to End IP **192.168.0.200**.
Domain Name	You can specify the Domain Name for your Access Point.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press "Continue" for configure other

settings or “Apply” to restart WRT-414 with new configuration.

5.4 Wireless

This screen allows you to Enable/Disable WRT-414 wireless function.

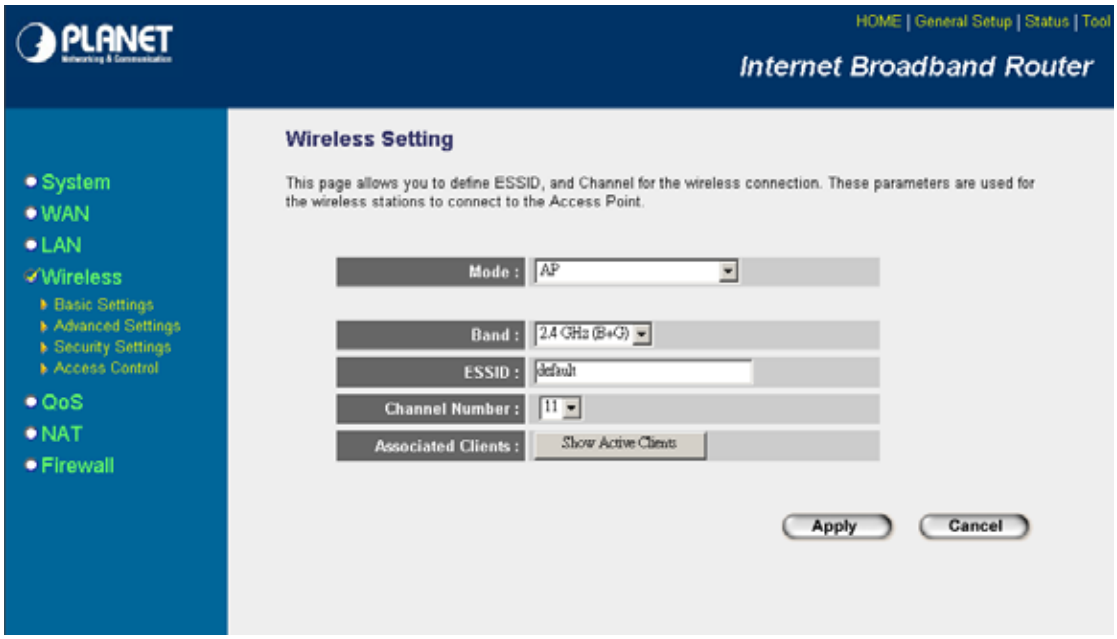


Parameters	Description
Enable/Disable	You can select to “**Enable**” or “**Disable**” the Wireless interface. After selected, please click “Apply” to make the settings effect.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

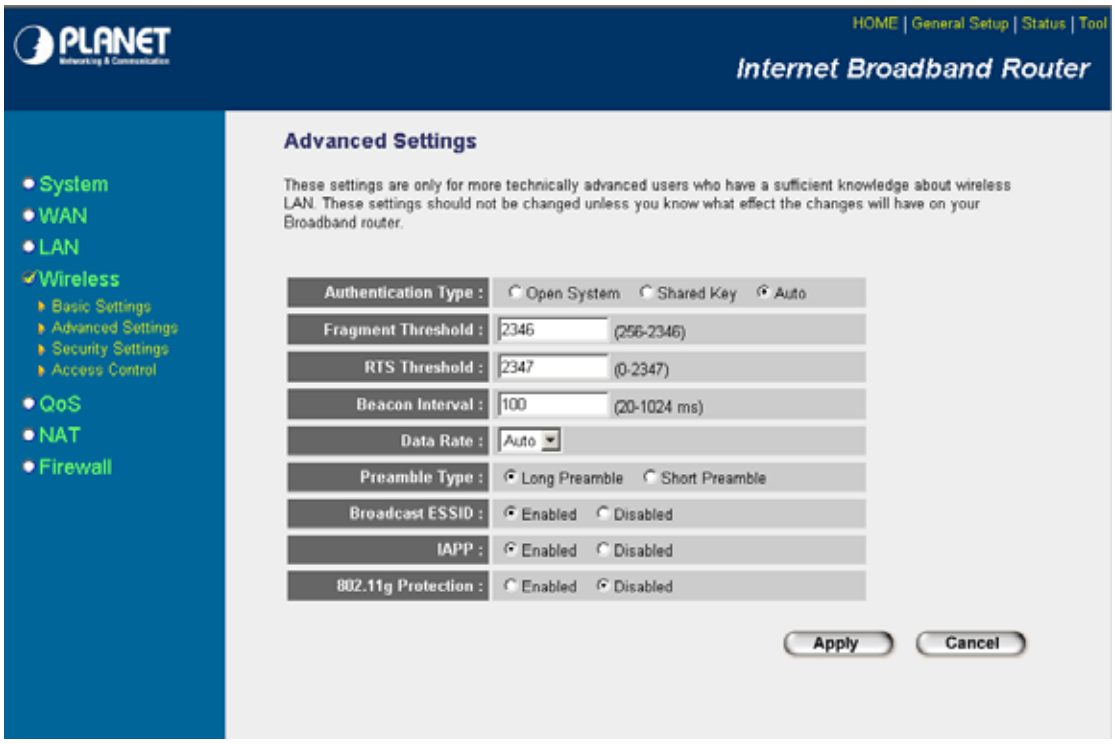
5.4.1 Basic Settings

WRT-414 supports not only Access Point function, but also provides Station, Bridge and WDS mode. Please Refer to **"Chapter 6 Wireless Configuration**" know the details settings of wireless Basic Settings. In Default, WRT-414 will work with AP mode.



5.4.2 Advance Settings

You should not change the parameters in this screen unless you know what effect the changes will have on WRT-414. When configuration finished, please click "Apply" to save the settings.



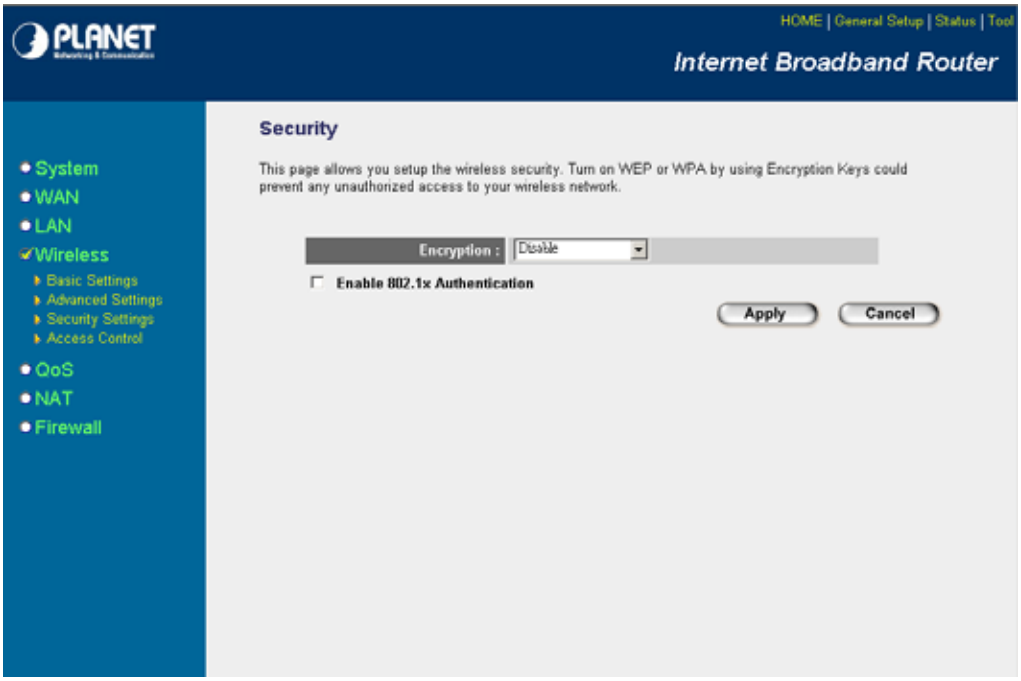
Parameters	Description
Authentication Type	Normally, you can leave this at “Auto”, so that Wireless Stations can use either method ("Open System" or "Shared Key".). If you wish to use a particular method, select the appropriate value - "Open System" or "Shared Key". All Wireless stations must then be set to use the same method.
Fragment Threshold	“Fragment Threshold” specifies the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller the RTS threshold, the access point will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	The interval of time that this access point broadcast a beacon. Beacon is used to synchronize the wireless network.
Data Rate	The Data Rate is the rate of data transmission. The WRT-414 will use the highest possible selected transmission rate to transmit the data packets.
Preamble Type	Preamble type defines the length of CRC block in the frames during the wireless communication. “**Short Preamble**” is suitable for high traffic wireless network. “**Long Preamble**” can provide more reliable communication.
Broadcast ESSID	If you enable “Broadcast ESSID”, every wireless station located within the coverage of this access point can discover this WRT-414 easily. If you are building a public wireless network, enabling this feature is recommended. In

	private network, disabling “Broadcast ESSID” can provide better security.
IAPP	If you enable “IAPP”, the access point will automatically broadcast information of associated wireless stations to its neighbors. This will help wireless station roaming smoothly between access points. If you have more than one access points in your wireless LAN and wireless stations have roaming requirements, enabling this feature is recommended. Disabling “IAPP” can provide better security.
802.11g Protection	This is also called CTS Protection. It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.4.3 Security

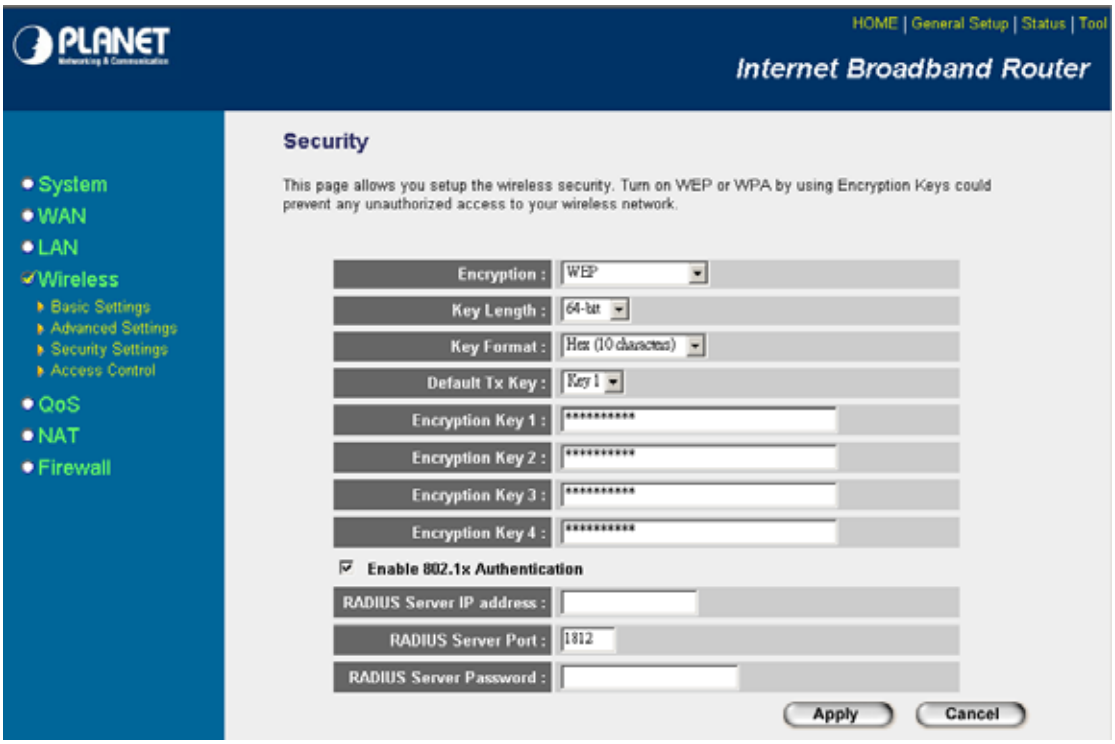
WRT-414 provides complete wireless LAN security functions, includes WEP, 802.1x, 802.1x with WEP, WPA-PSK and WPA RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function. In default, the security function is “Disable”.



5.4.3.1 WEP

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself. You can enter four WEP keys and select one of them as default key. Then the access point will just allow the clients that with the same encryption keys connected. You can use WEP encryption in “AP mode”, “Station-Ad Hoc mode”, “Station-Infrastructure mode” and “AP Bridge-WDS mode”.

If you would like to enable 802.1x Authentication also, please check the “Enable 802.1x Authentication” and refer to section 5.4.3.2 for the detail of 802.1x settings.



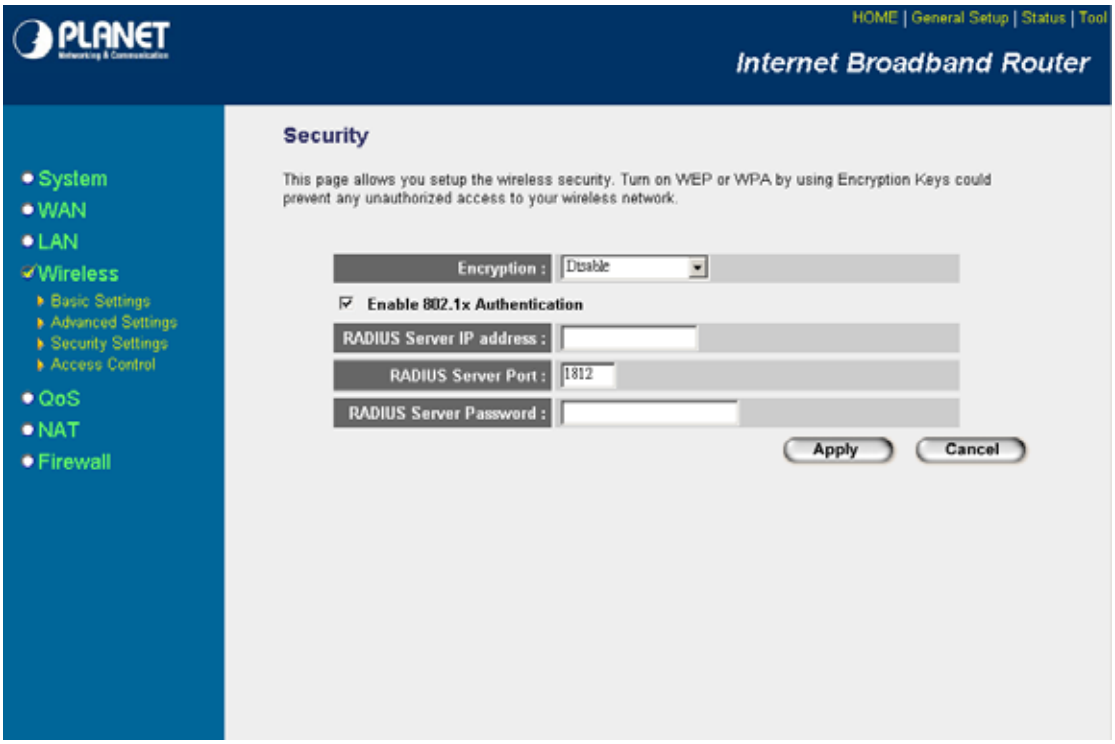
Parameter	Description
Encryption	Please select “WEP” in this option.
Key Length	You can select the 64 or 128-bit key to encrypt transmitted data. Larger WEP key length will provide higher level of security, but the throughput will be lower.
Key Format	You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the WEP Key.
Default Tx Key	Select one of the four keys to encrypt your data. Only the key you select it in the “Default key” will take effect.
Encryption Key 1 - Key 4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII character as the encryption keys.

	128-bit WEP: input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 10-digit ASCII characters as the encryption keys.
Enable 802.1x Authentication	Check this box if you want to enable 802.1x authentication with WEP encryption. You may refer to section 5.4.3.2 to enter the correct setting of the fields.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.4.3.2 802.1x

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication. It is suggested to enable 802.1x and WEP at the same time.

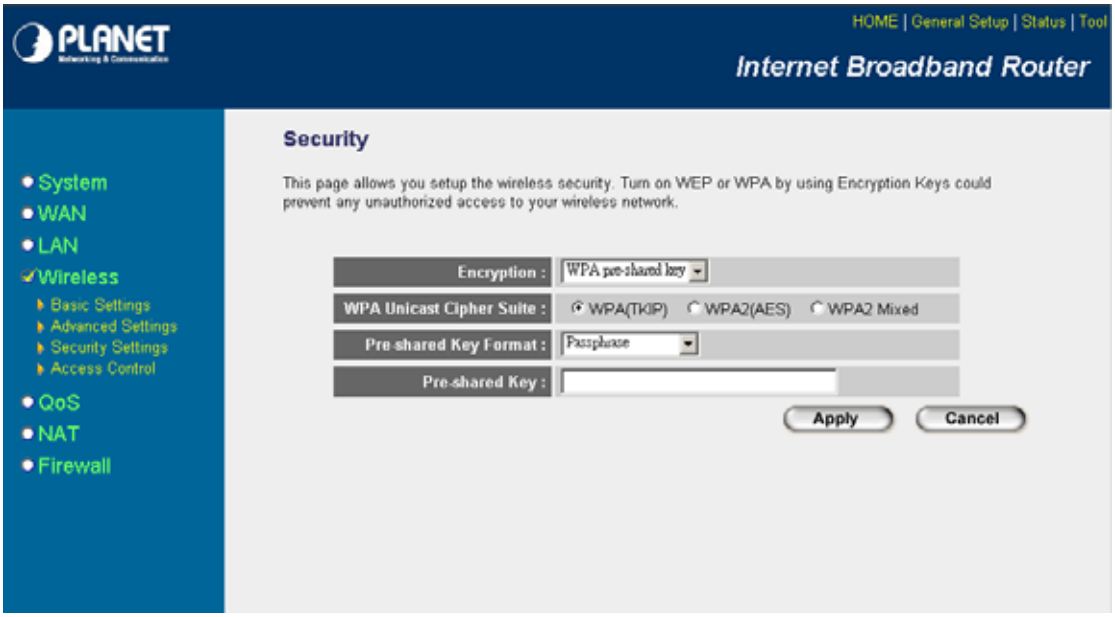


Parameter	Description
Encryption	If you want to use 802.1x only, keep this setting in “Disable”.
Enable 802.1x Authentication	Please check this option to enable 802.1x function.
RADIUS Server IP Address	Enter RADIUS Serer IP address.
RADIUS Server Port	Leave the default port setting or assign a new port number for this option.
RADIUS Server Password	Please enter the password that is configured in RADIUS Server.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.4.3.3 WPA-PSK

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.



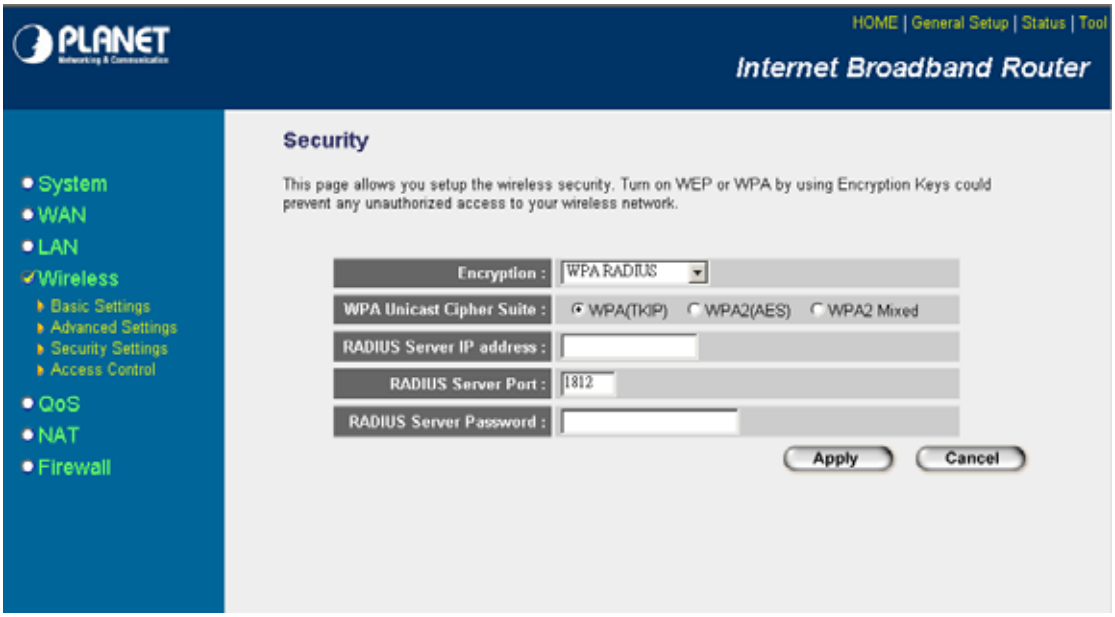
Parameter		Description
Encryption		Please select “WPA pre-shared key” in this option.
WPA Unicast Cipher Suite	WPA (TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
	WPA2 (AES)	This use CCMP protocol to change encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
	WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
Pre-shared Key Format		You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key.
Pre-shared Key		The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below.

	Hex: input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.4.3.4 WPA RADIUS

You can use a RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently.

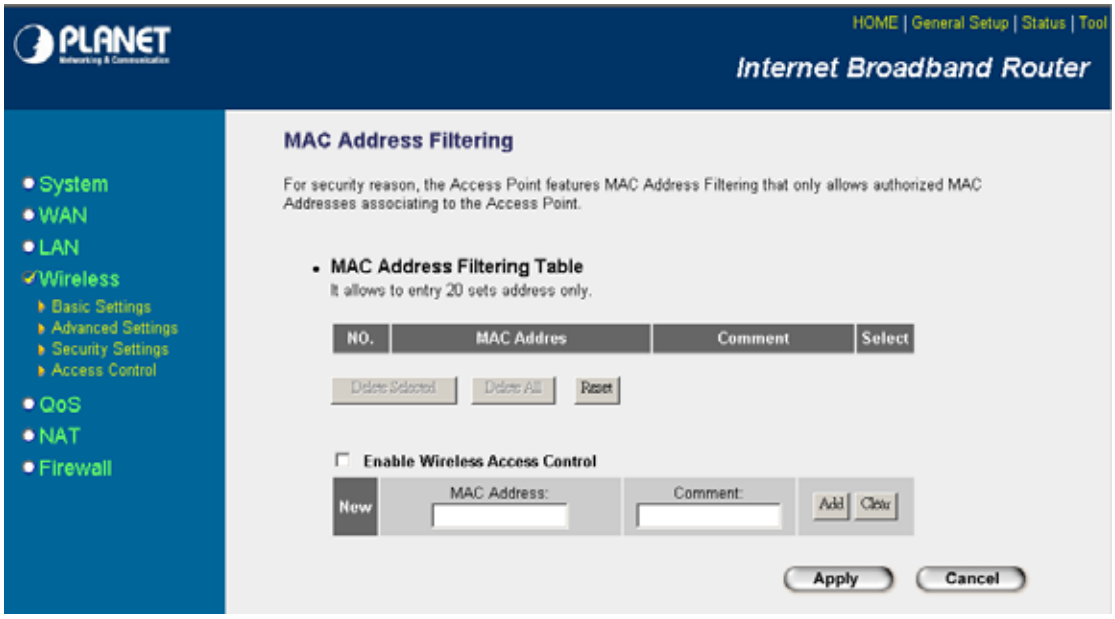


Parameter		Description
Encryption		Please select “WPA RADIUS” in this option.
WPA Unicast Cipher Suite	WPA (TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
	WPA2 (AES)	This use CCMP protocol to change encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
	WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
RADIUS Server IP Address		Enter RADIUS Serer IP address.
RADIUS Server Port		Leave the default port setting or assign a new port number for this option.
RADIUS Server Password		Please enter the password that is assigned in RADIUS Server.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.4.4 Access Control

WRT-414 provides MAC Address Filtering, which prevents the unauthorized users from accessing your wireless network.



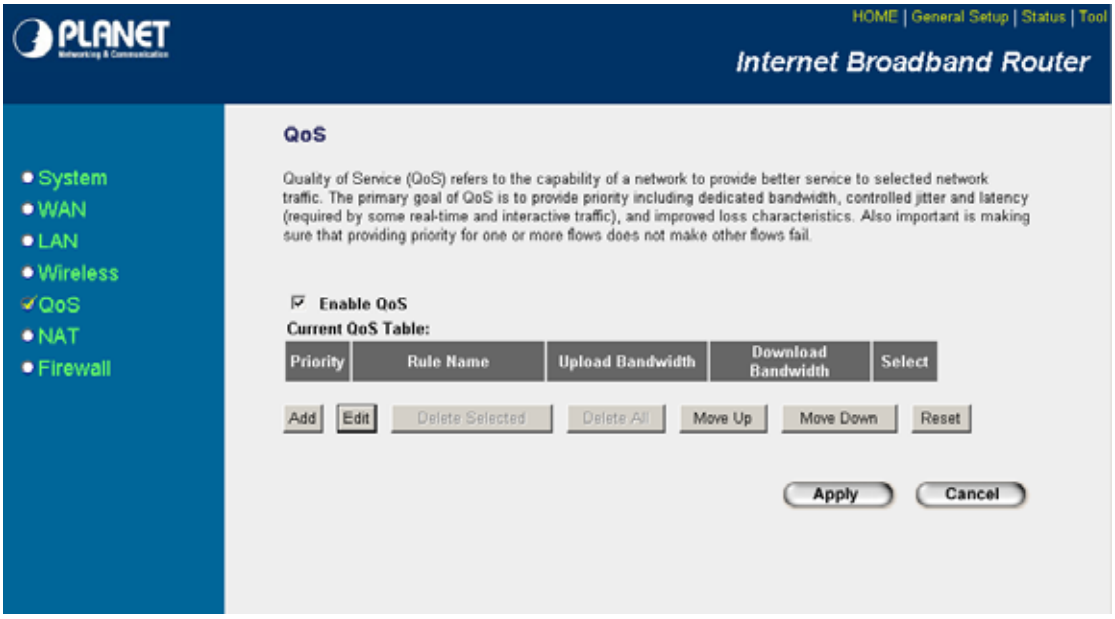
Parameters	Description
Enable Wireless Access Control	Enable or disable the MAC Address Filtering function.
Add MAC Address to the control table	In the bottom “New” area, fill in the “MAC Address” and “Comment” of the wireless station and then click “Add”. Then this wireless station will be added into the “MAC Address Filtering Table” above.
Remove MAC address from the table	If you want to remove some MAC address from the “Current Access Control List”, select the MAC addresses you want to remove in the list and then click “Delete Selected”.
Delete All	If you want remove all MAC addresses from the list, just click this button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.5 QoS

Quality of Service (QoS) refers to the capability of providing better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. When using this

feature, it is important to make sure the rules are not conflicted with each other.



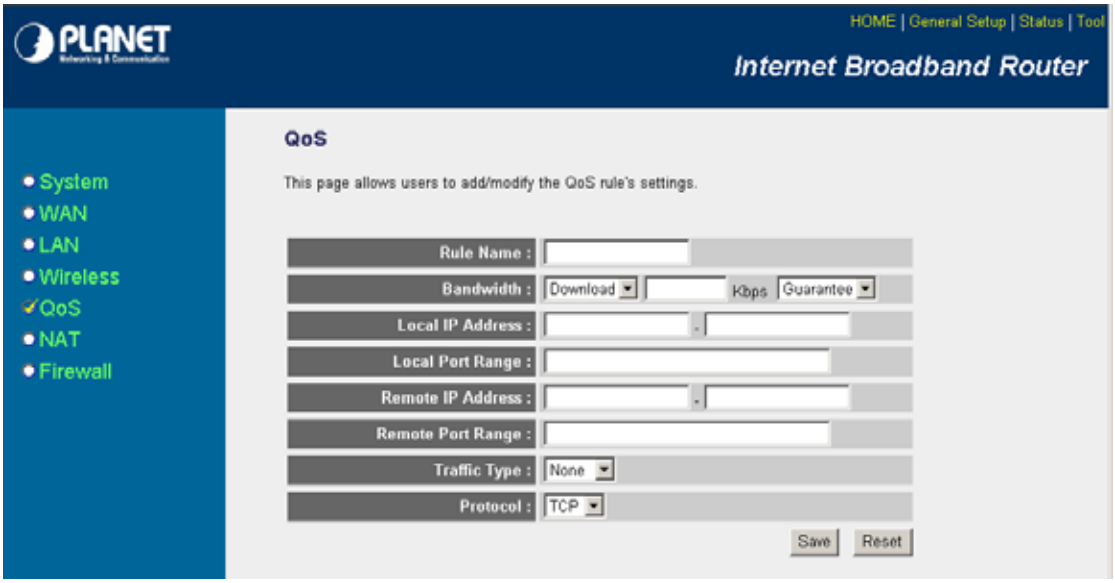
Parameters	Description
Add	When you want to add a new QoS rule, press this button and refer to section 5.5.1 to add a new QoS rule.
Edit	When you want to edit the existing QoS rule, press this button and refer to section 5.5.1 to edit QoS rule.
Delete Selected	Select the QoS rule which you would like to delete , then press this button to delete.
Delete All	When you want to delete all the QoS rules, you just need to press this button.
Move Up	Select a QoS rule and press this button to assign higher priority.
Remove Down	Select a QoS rule and press this button to assign lower priority.
Reset	Click “Reset” to clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.5.1 Add/Edit QoS Rule

You can assign packet classification criteria by its source IP range, destination IP range, traffic type, protocol, source port range and destination port range parameters. The parameters that you leave as blank will be ignored. The priority of this rule will be applied to packets that match classification criteria of this rule. You can limit bandwidth consumed by packets that match this rule or guarantee bandwidth required by packets that match this rule.

After press Add or Edit button in QoS screen, you will see the web screen below for user to setup their QoS rule.

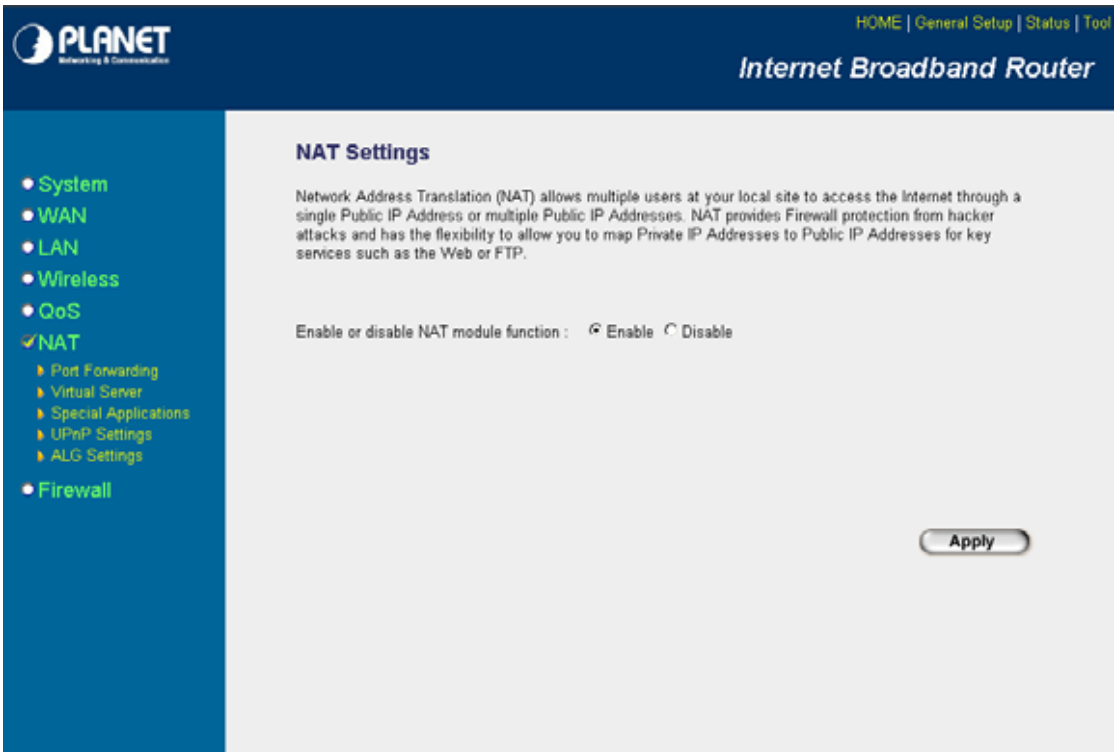


Parameters	Description
Rule Name	Please give a name to the QoS Rule
Bandwidth	You can limit the maximum bandwidth consumed by this rule by selecting “Maximum”. You also can reserve enough bandwidth for this rule by selecting “Guarantee”. The unit of bandwidth is Kbps. When we download data from Internet, the unit of download screen shows is KBps. 1KBps is equal to 8Kbps. When you enter the bandwidth, please make sure the number you enter is correct. For example, if you want to limit users download speed to 50KBps from Internet, you will need to enter 400Kbps in the configuration.
Local IP Address	Please enter the IP address of the local PC.
Local Port Range	Please enter the port range.
Remote IP Address	Please enter the IP address of the PC from remote site.
Remote Port Range	Please enter the port range.
Traffic Type	Select the traffic type of the packets that this rule will apply to. We list some popular applications here to ease the configuration. You also can get the same result by using other parameters, for example source or destination port number, if you are familiar with the application protocol.
Protocol	Please select the protocol TCP or UDP in the list.

After configuration complete, please click “Save” to save the settings. Or you may press “Reset” to clear the settings to enter again.

5.6 NAT

Network Address Translation (NAT) allows multiple users at your local site to access the Internet via a single legal IP Address. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. If NAT is disabled, all LAN side workstations must have legal IP addresses for Internet access. If the router is used for routing application, not for Internet access, the NAT function can be disabled.

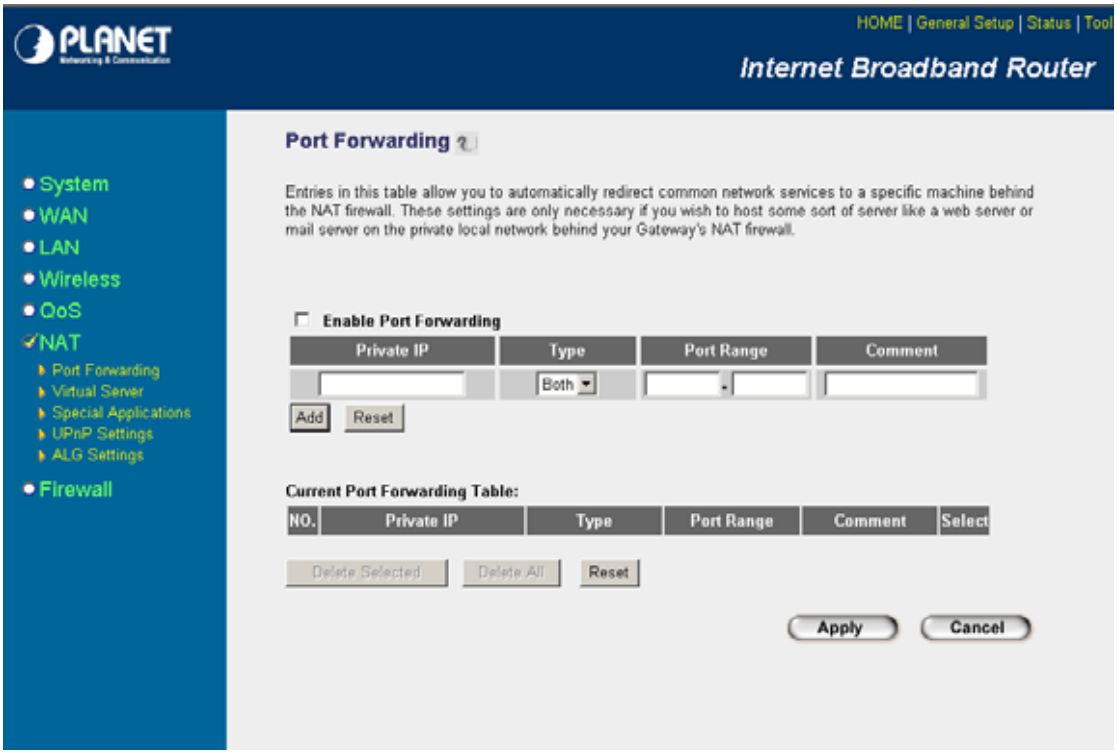


Parameters	Description
Enable/Disable	You can select to enable or disable the NAT function. After selected, please click “Apply” to make the settings effect.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.6.1 Port Forwarding

The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the firewall.



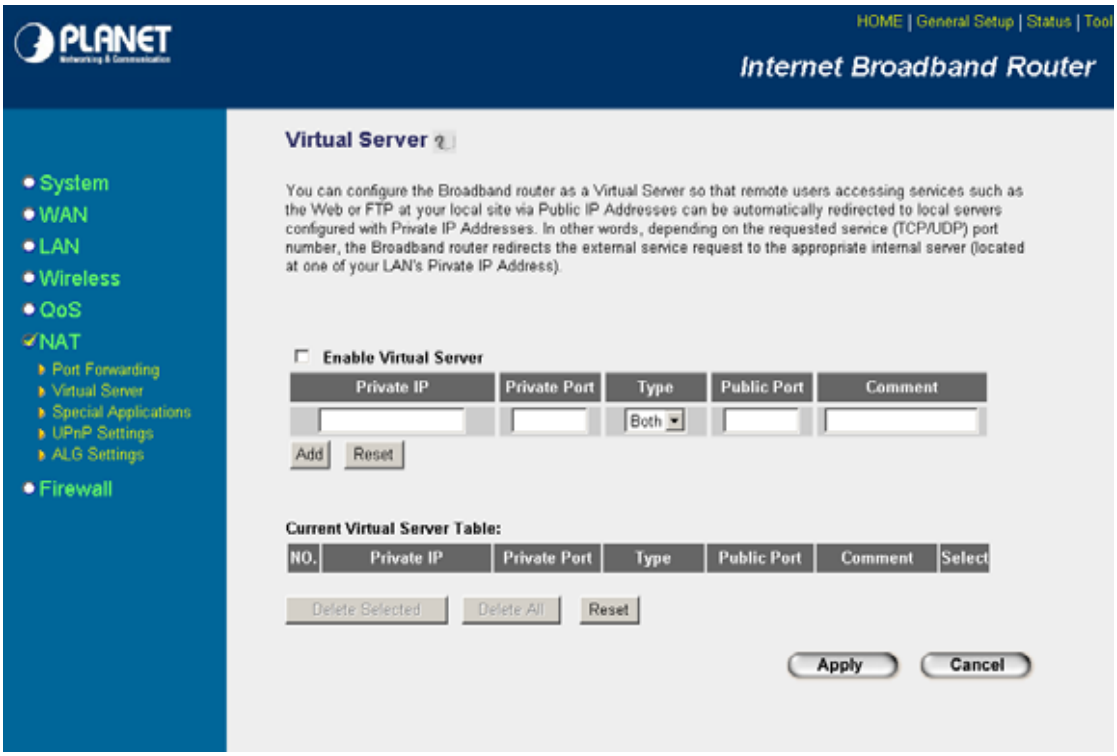
Parameters	Description
Enable Port Forwarding	Enable Port Forwarding.
Private IP	This is the private IP of the server in LAN. **Note:** You need to give your LAN PC clients a fixed/static IP address for Port Forwarding to work properly.
Type	This is the protocol type to be forwarded. You can choose to forward “TCP” or “UDP” packets only or select “both” to forward both “TCP” and “UDP” packets.
Port Range	The range of ports to be forward to the private IP.
Comment	The description of this setting.
Add	Fill in the "Private IP", “Type”, “Port Range” and "Comment" of the setting to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below. If you find any typo before adding it and want to retype again, just click "Clear" and the fields will be cleared.
Reset	Click “Reset” will clear your current settings to allows you to enter again.

Current Port Forwarding Table	
Delete Selected	If you want to remove some MAC address from the “Current Access Control List”, select the MAC addresses you want to remove in the table and then click “Delete Selected”.
Delete All	If you want remove all MAC addresses from the table, just click this button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.6.2 Virtual Server

Use the Virtual Server function when you need to have different servers in your LAN to handle many services and Internet applications (e.g. Email, FTP, Web server etc.) to the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the WAN Port) to a particular LAN private IP address as its service port number. (See Glossary for an explanation on Port number).



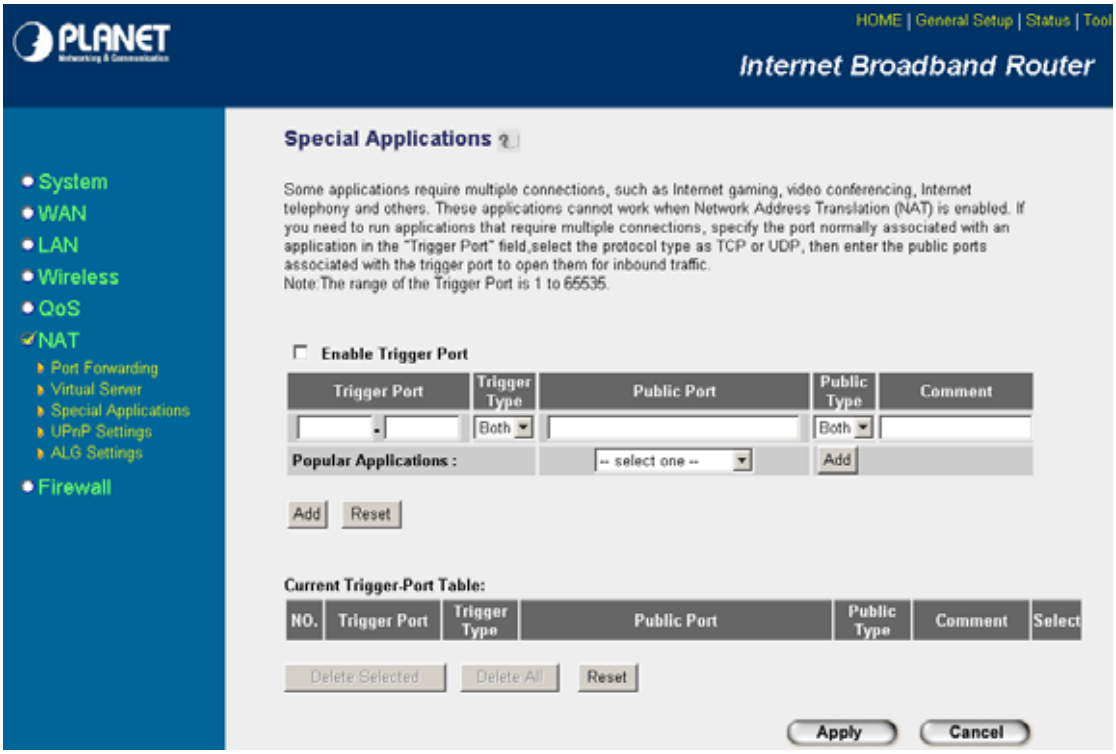
Parameters	Description
Enable Virtual Server	Enable Virtual Server.
Private IP	This is the LAN client/host IP address that the Public Port number packet will be sent to.

	Note: You need to give your LAN PC clients a fixed/static IP address for Virtual Server to work properly.
Private Port	This is the port number (of the above Private IP host) that the below Public Port number will be changed to when the packet enters your LAN (to the LAN Server/Client IP).
Type	Select the port number protocol type (**TCP**, **UDP** or **Both**). If you are unsure, then leave it to the default both protocols.
Public Port	Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN. **Note:** Virtual Server function will have priority over the DMZ function if there is a conflict between the Virtual Server and the DMZ settings.
Add	Fill in the "Private IP", "Private Port", "Type", “Public Port” and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below. If you find any typo before adding it and want to retype again, just click "Clear" and the fields will be cleared.
Reset	Click “Reset” will clear your current settings to allows you to enter again.
Current Virtual Server Table	
Delete Selected	If you want to remove some items from the “Current Virtual Server Table”, select the MAC addresses you want to remove in the table and then click “Delete Selected”.
Delete All	If you want remove all items of the table, just click this button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.6.3 Special Applications

Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.



Parameters	Description
Enable Trigger Port	Enable the Special Application function.
Trigger Port	This is the out going (Outbound) range of port numbers for this particular application.
Trigger Type	Select whether the outbound port protocol are "**TCP**", "**UDP**" or "**Both**".
Public Port	Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624). **Note:** Individual port numbers are separated by a comma (e.g. 47624, 5775, 6541 etc.). To input a port range use a "dash" to separate the two port number range (e.g. 2300-2400).
Public Type	Select the Inbound port protocol type: "TCP", "UDP" or both.
Comment	The description of this setting.
Popular applications	This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, click the "Add" button in right side of this setting. This will automatically copy the Port Trigger information required

	for this popular application into the input fields.
Add	Add the settings into the “Current Trigger Port Table”.
Reset	Click “Reset” will clear your current settings to allows you to enter again.
Current Trigger Port Table	
Delete Selected	If you want to remove some items from the “Current Trigger Port Table”, select the MAC addresses you want to remove in the table and then click “Delete Selected”.
Delete All	If you want to remove all items from the table, just click this button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

Example: Special Applications

If you need to run applications that require multiple connections, specify the port (outbound) normally associated with that application in the "Trigger Port" field. Then select the protocol type (TCP or UDP) and enter the public ports associated with the trigger port to open them up for inbound traffic.

Example:

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624	TCP	MSN Game Zone
2	6112	UDP	6112	UDP	Battle.net

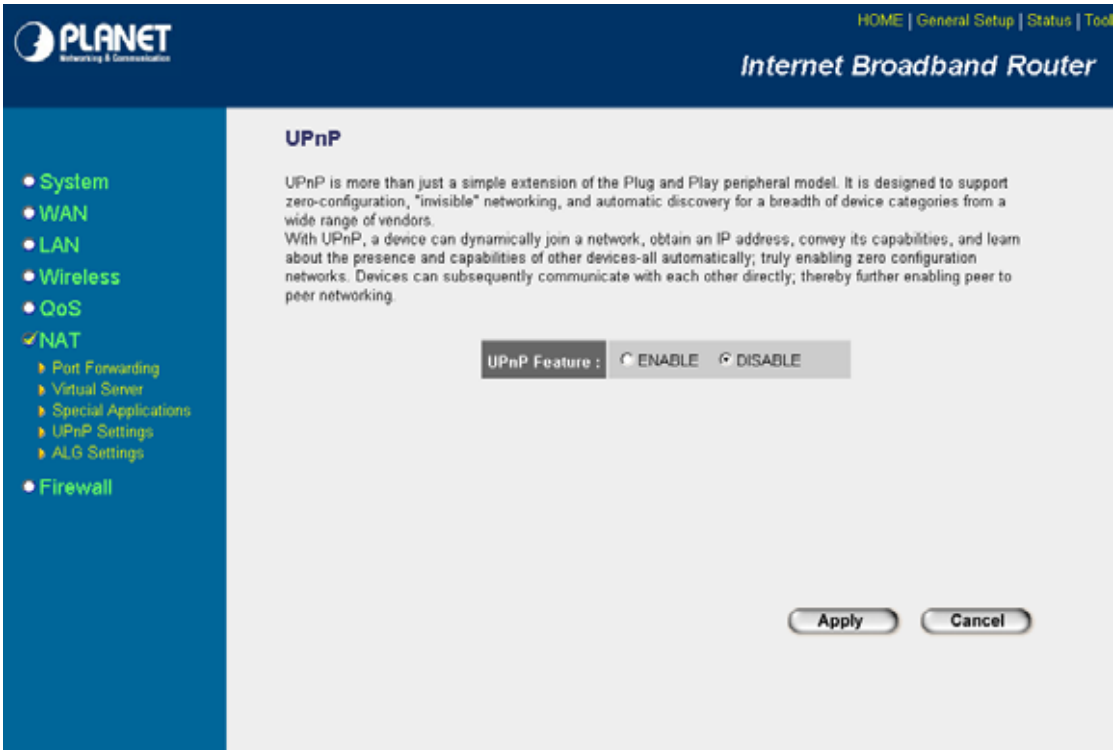
In the example above, when a user trigger’s port 28800 (outbound) for MSN Game Zone then the router will allow incoming packets for ports 2300-2400 and 47624 to be directed to that user.

Note: Only one LAN client can use a particular special application at a time.

5.6.4 UPnP

UPnP is more than just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors.

With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices-all automatically; truly enabling zero configuration networks. Devices can subsequently communicate with each other directly; thereby further enabling peer to peer networking.

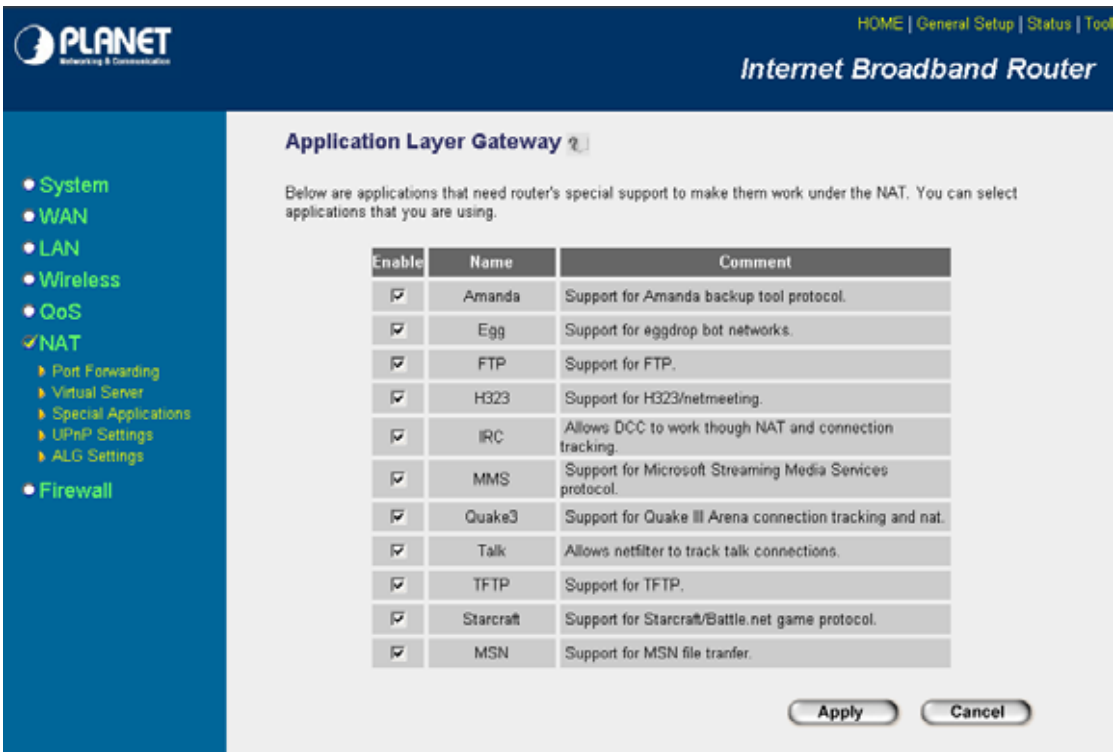


Parameters	Description
UPnP Feature	Enable or Disable UPnP function.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.6.5 ALG Settings

You can select applications that need “Application Layer Gateway” to support.

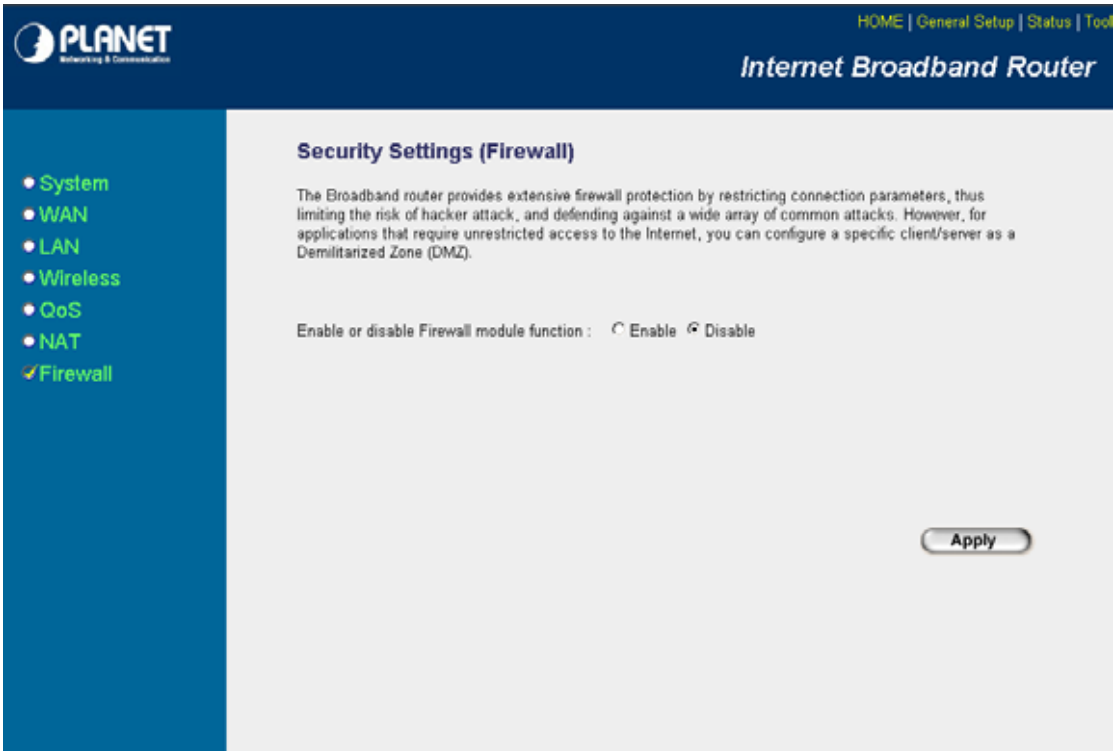


Parameters	Description
Enable	You can select to enable “Application Layer Gateway” of an application and then the router will let that application correctly pass though the NAT gateway.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.7 Firewall

WRT-414 provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server in a Demilitarized Zone (DMZ).

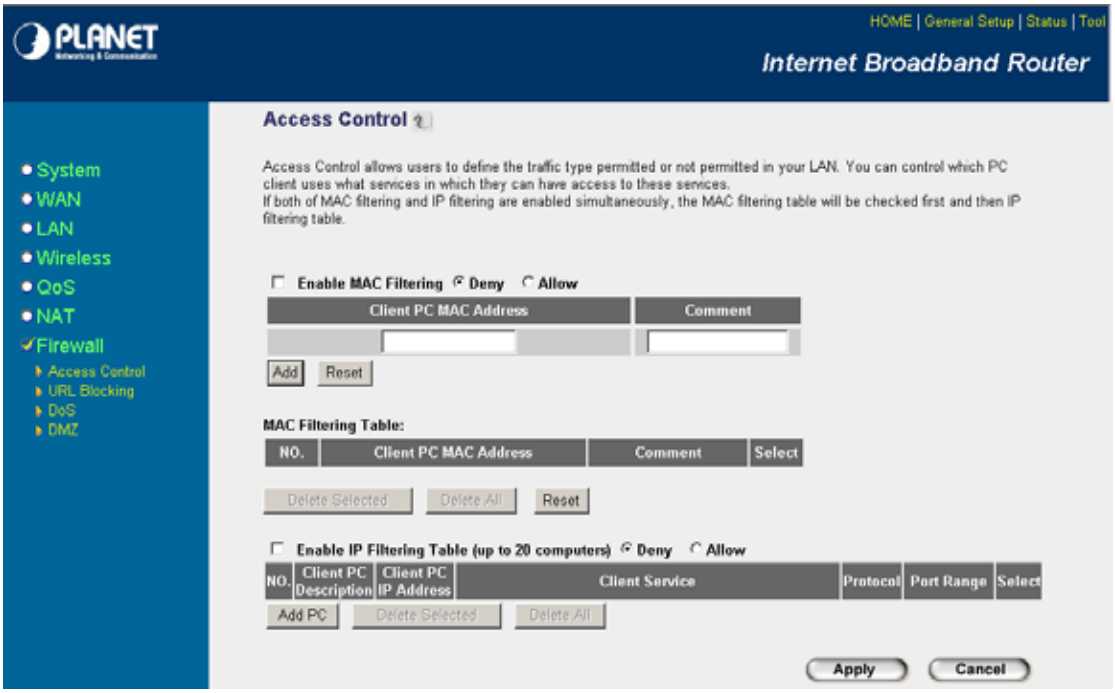


Parameters	Description
Enable/Disable	You can select to enable or disable the firewall function. After selected, please click “Apply” to make the settings effect.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.7.1 Access Control

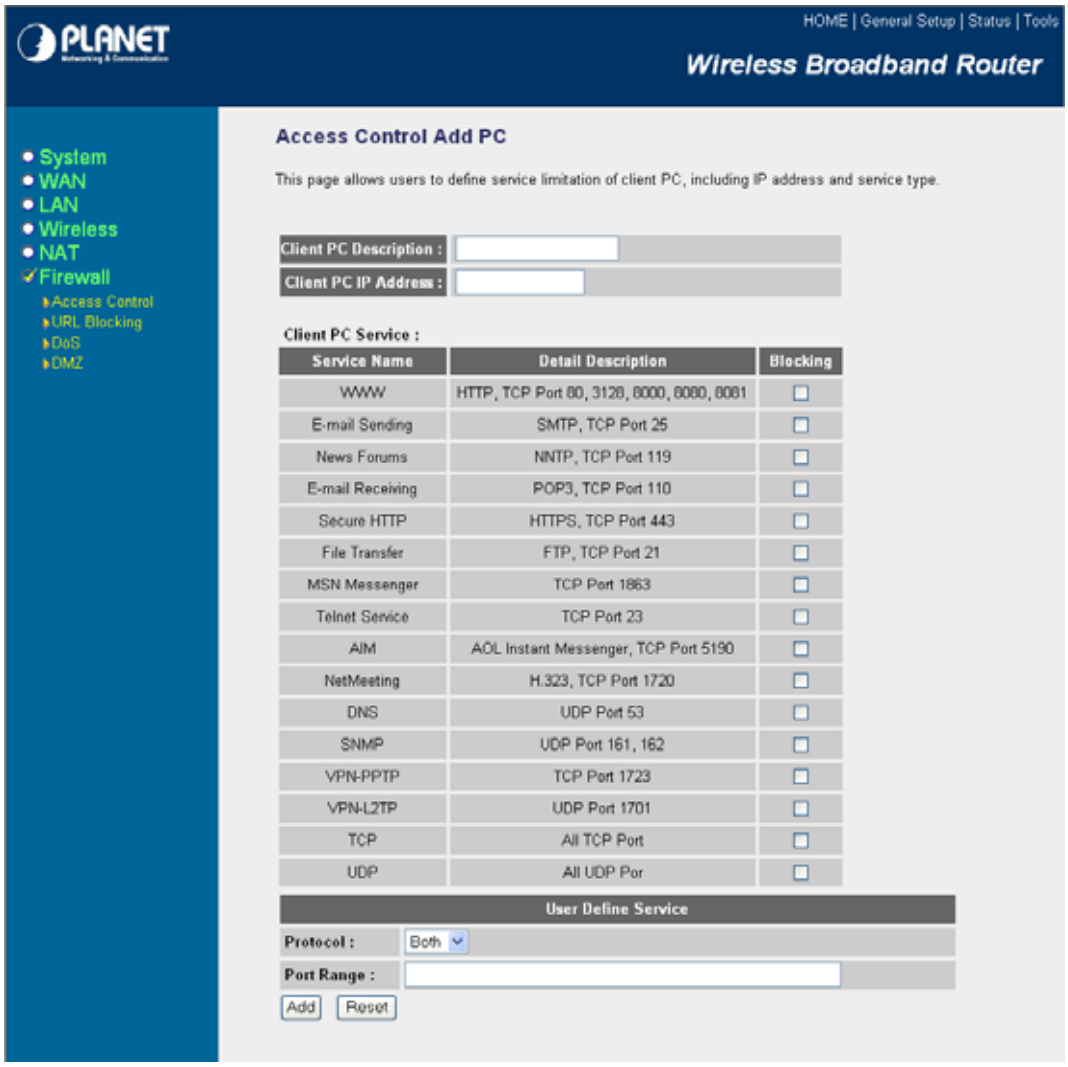
This screen allows you to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.). Network administrator can define the traffic type permitted in your LAN and control which PC client can have access to these services.



Parameters	Description
Enable MAC Filtering	Check “Enable MAC Filtering” to enable MAC Filtering. If select “Deny”, all PCs will be allowed to access Internet accept for the PCs in the list below. If select “Allow”, all PCs will be denied to access Internet accept for the PCs in the list below.
Add PC	Fill in “Client PC MAC Address” and “Comment” of the PC that is allowed to access the Internet, and then click “Add”. If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.
Remove PC	If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want remove all PCs from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.
Enable IP Filtering Table	Check “Enable IP Filtering Table” to enable IP filter. If select “Deny”, all PCs will be allowed to access Internet accept for the PCs in the list below. If select “Allow”, all PCs will be denied to access Internet accept for the PCs

	in the list below.
Add PC	You can click “Add PC” to add an access control rule for users by IP addresses. Please refer to section 5.7.1.1.
Remove PC	If you want to remove some PCs from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected".
Delete All	If you want to delete all PCs. Please click this button.

5.7.1.1 Add PC



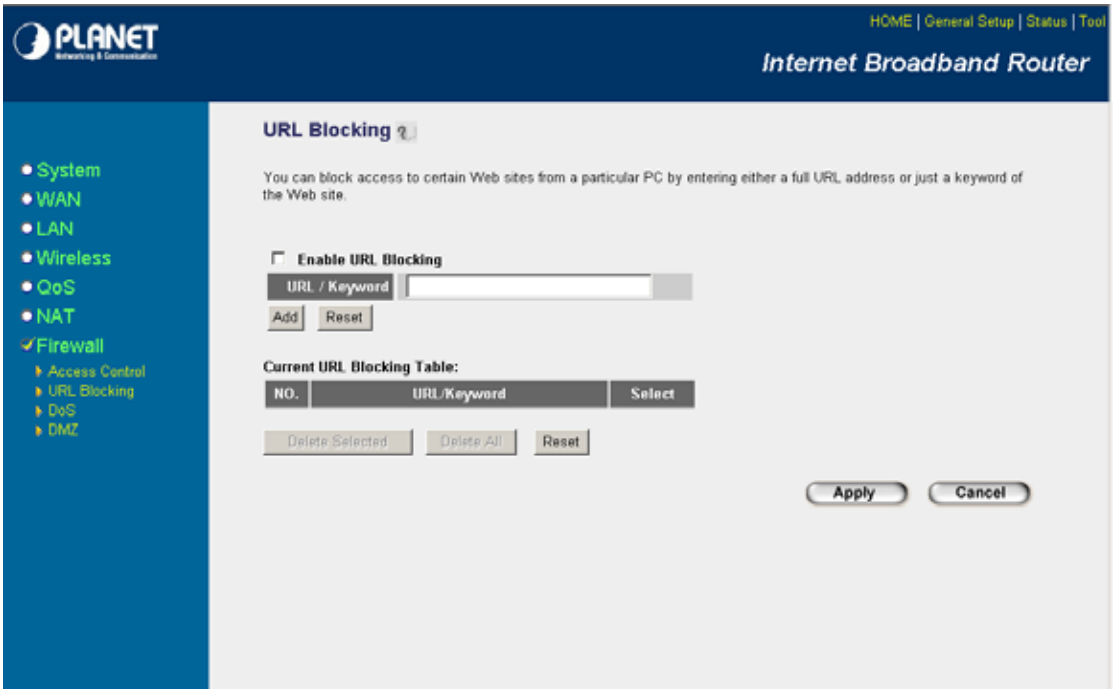
Parameters	Description
Client PC Description	The description for this client PC.
Client PC IP Addresses	Enter the IP address range that you wish to apply this Access Control rule. You can select a range of users simply by inputting the starting users’ IP address and the last user’s IP address in the appropriate boxes. If you want to select only one user, just input the user’s IP address in both boxes.

	Note: You need to give your LAN PC clients a fixed/static IP address for the Access Control rule to work properly.
Client PC Service	You can block the clients from accessing some Internet services by checking the services you want to block.
Protocol	This allows you to select **UDP**, **TCP** or **Both** protocol types.
Port Range	You can assign up to five port ranges. The router will block clients from accessing Internet services that use these ports.
Add	Click “Add” to save the settings.
Reset	Click “Reset” to clear all fields.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.7.2 URL Blocking

You can block users to access to some web sites by entering a full URL address or just keyword of the web site.



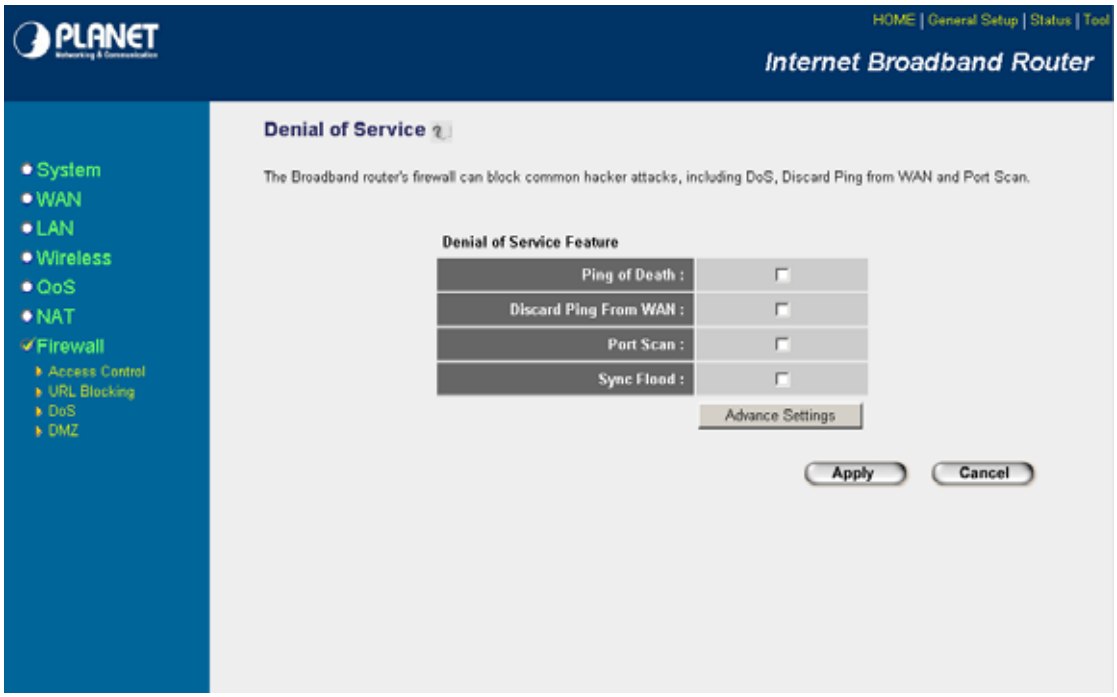
Parameters	Description
Enable URL Blocking	Enable/disable URL Blocking.
Add URL / Keyword	Fill in “URL / Keyword” and then click “Add”. You can enter the full URL address or the keyword of the web site you want to block. If you find any typo before adding it and want to retype again, just click "Reset" and the field will

	be cleared.
Remove URL / Keyword	If you want to remove some URL keyword from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keyword from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.7.3 DoS

WRT-414's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur, the router can log the events.

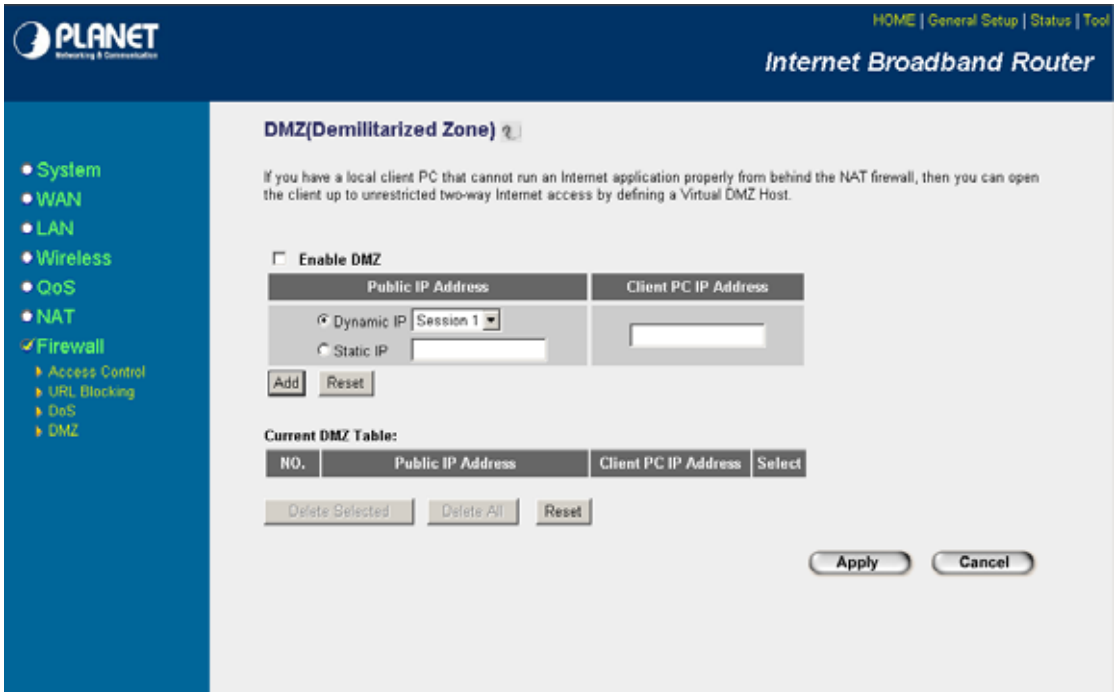


Parameters	Description
Ping of Death	Protections from Ping of Death attack.
Discard Ping From WAN	The router’s WAN port will not respond to any Ping requests.
Port Scan	Protects the router from Port Scan.
Sync Flood	Protects the router from Sync Flood attack.
Advance Settings	If you want to configure the details of each setting above, click this button, and you will see the detail configure screen. Please make sure what the effect of the settings will affect before your adjustment.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

5.7.4 DMZ

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets from your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) to one particular LAN client/server.

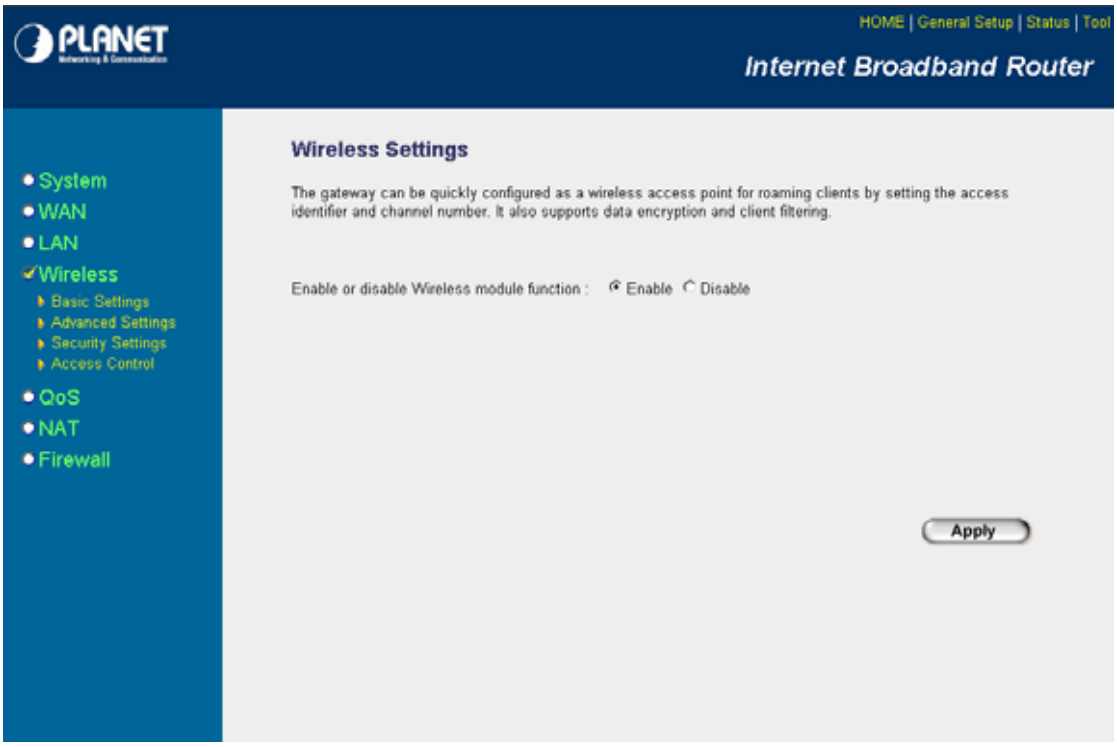


Parameters	Description
Enable DMZ	Enable/disable DMZ. **Note:** If there is a conflict between the Virtual Server and the DMZ setting, the Virtual Server function will have priority over the DMZ function.
Public IP Address	The IP address of the WAN port or any other Public IP addresses given to you by your ISP.
Client PC IP Address	Input the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above. **Note:** You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

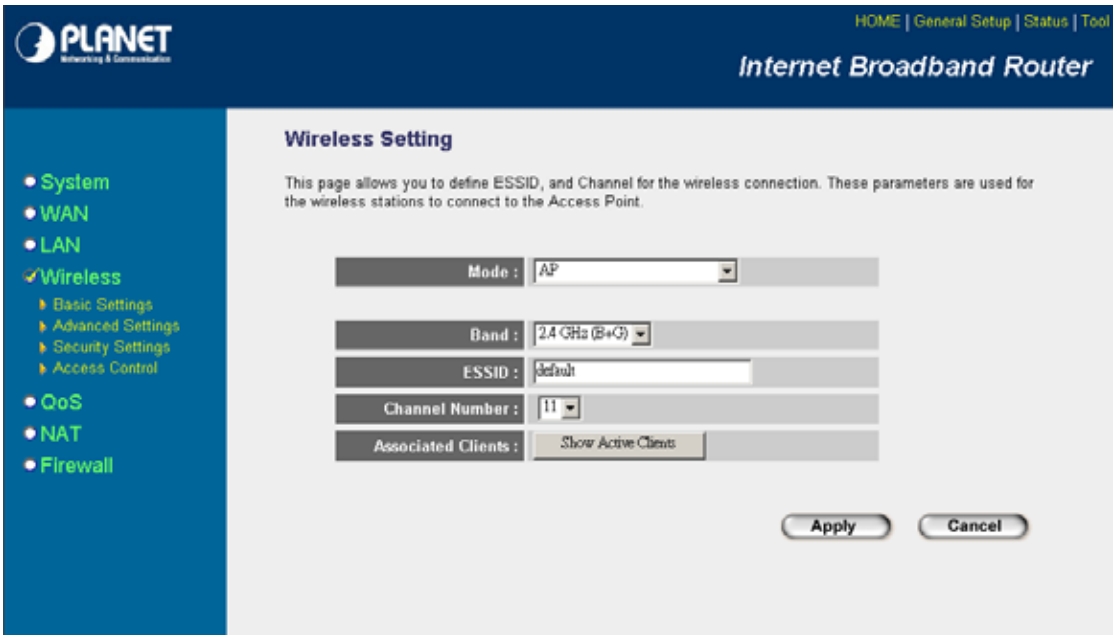
Chapter 6 Wireless Configuration

In this chapter, you can Enable/Disable wireless function and configure the WRT-414 work in different operating mode. Please refer to below sections to know the details configuration of each operating mode.



6.1 AP Mode

This mode is set to WRT-414 by default. It served as a transparent Media Access Control (MAC) bridge between wired and wireless network.



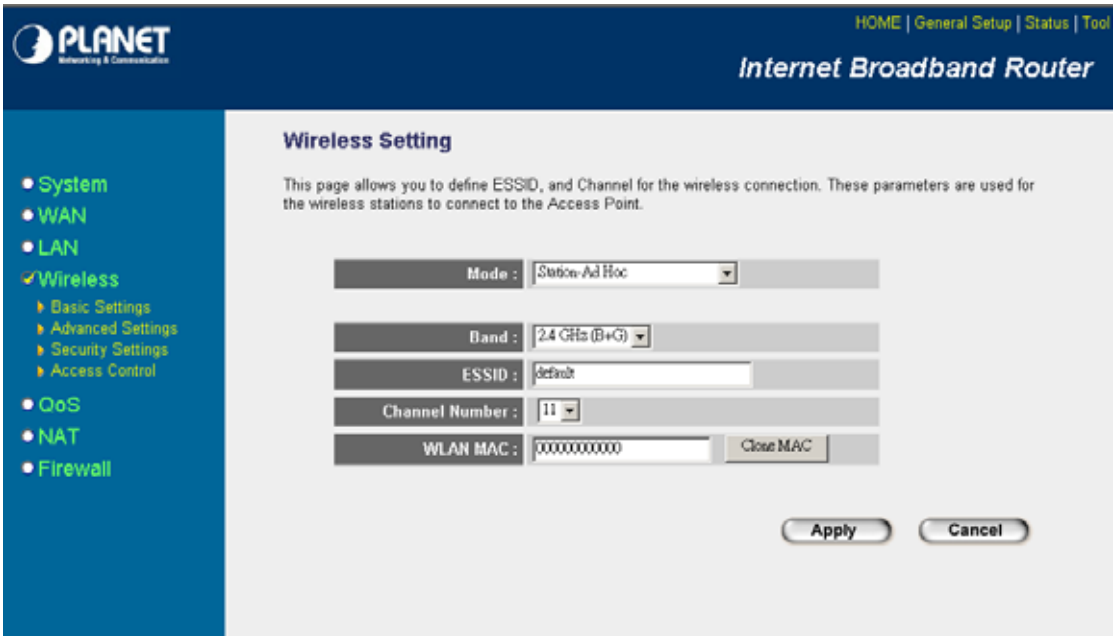
Parameter	Description
Mode	Shows the current operation mode. You may set WRT-414 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It forces the WRT-414 to operate in 802.11b only. **2.4GHz (G):** It forces the WRT-414 to operate in 802.11g only. **2.4GHz (B+G):** It allows the WRT-414 to operate in 802.11b and 802.11g simultaneously.
ESSID	The ESSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Please make sure that the ESSID of all stations in the same WLAN network are the same. The default value is "**default**".
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
Associated Clients	You may press "**Show Active Clients**" button to check the connected client information. After the button pressed, you will see the dialog box as below.

You may press "**Refresh**" to get the new client table or "**Close**" to close this dialog box.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press "Continue" for configure other settings or "Apply" to restart WRT-414 with new configuration.

6.2 Station - Ad Hoc Mode

WRT-414 serves as a wireless station (Ad-hoc) in this mode. Connected to a PC or a small LAN (no more than 5 PCs), this station along with other wireless stations can establish a small wireless network without Access Points.

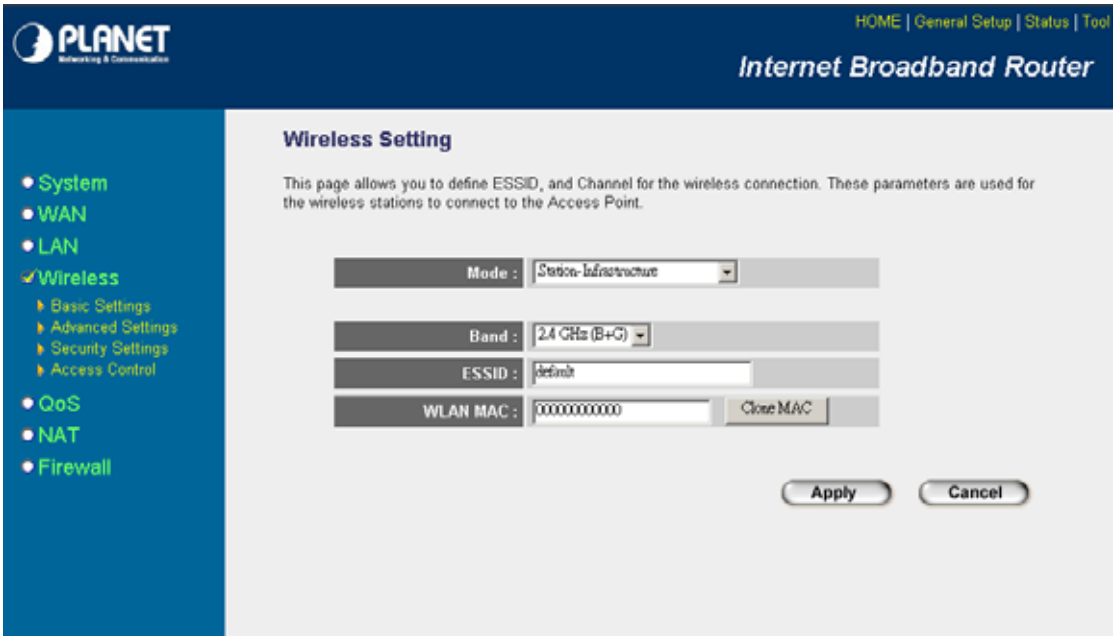


Parameter	Description
Mode	Shows the current operation mode. You may set WRT-414 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It forces the WRT-414 to operate in 802.11b only. **2.4GHz (G):** It forces the WRT-414 to operate in 802.11g only. **2.4GHz (B+G):** It allows the WRT-414 to operate in 802.11b and 802.11g simultaneously.
ESSID	Please make sure the ESSID of the wireless network that you will connected and enter the correct ESSID in this field. The default value is "**default**".
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
WLAN MAC	**Keep default setting**: WRT-414 will use it's own MAC address to access the wireless LAN. **Press "MAC Clone" button**: It will use PC's MAC address to access the wireless LAN.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press "Continue" for configure other settings or "Apply" to restart WRT-414 with new configuration.

6.3 Station - Infrastructure Mode

WRT-414 serves as a wireless station (infrastructure). Connected to a PC or a small LAN (no more than 5 PCs), it allows the PC or small LAN able to access the wireless network via Access Point.

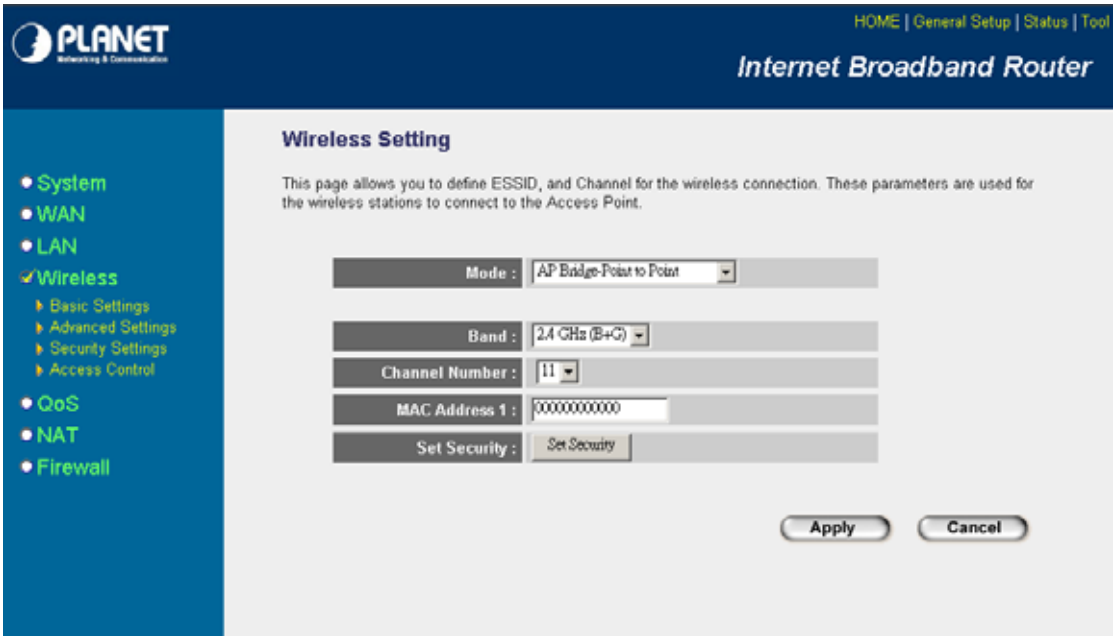


Parameter	Description
Mode	Shows the current operation mode. You may set WRT-414 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It forces the WRT-414 to operate in 802.11b only. **2.4GHz (G):** It forces the WRT-414 to operate in 802.11g only. **2.4GHz (B+G):** It allows the WRT-414 to operate in 802.11b and 802.11g simultaneously.
ESSID	Please make sure the ESSID of the wireless network that you will connected and enter the correct ESSID in this field. The default value is "**default**".
WLAN MAC	**Keep default setting**: WRT-414 will use it's own MAC address to access the wireless LAN. **Press "MAC Clone" button**: It will use PC's MAC address to access the wireless LAN.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press "Continue" for configure other settings or "Apply" to restart WRT-414 with new configuration.

6.4 AP Bridge - Point to Point Mode

This function allows WRT-414 to bridge 2 wired Ethernet networks wirelessly.

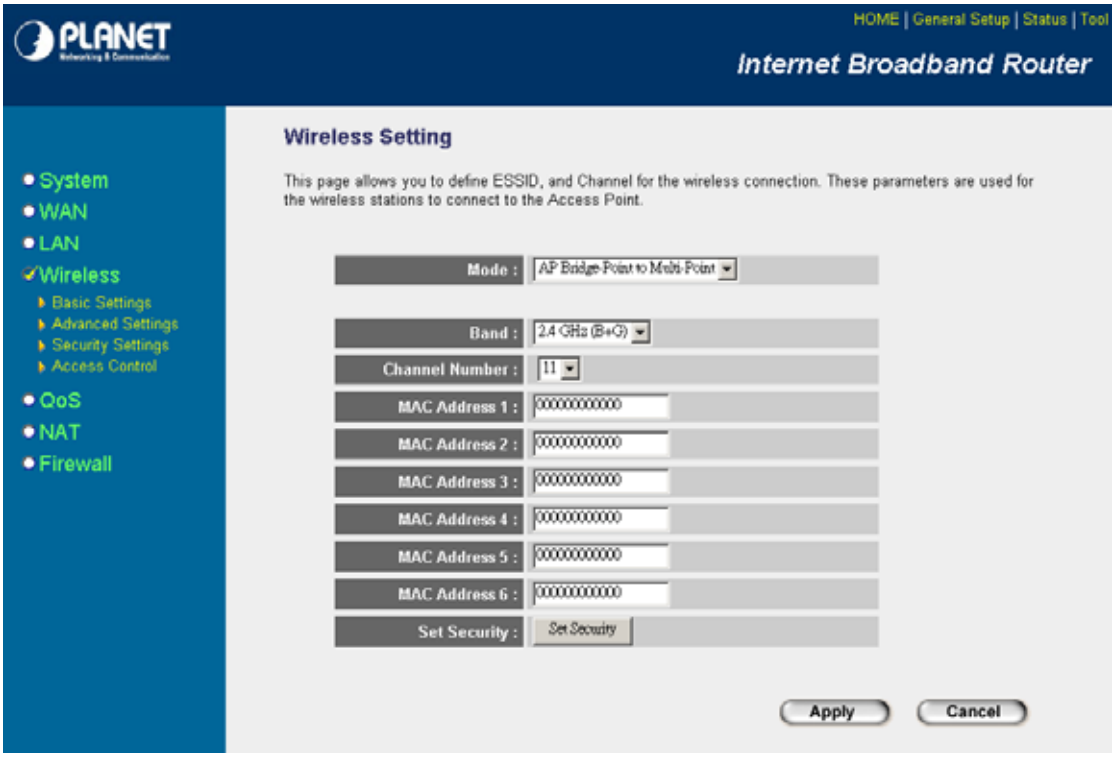


Parameter	Description
Mode	Shows the current operation mode. You may set WRT-414 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It allows to select the transmit rate up to 11Mbps. **2.4GHz (G):** It allows to select the transmit rate up to 54Mbps. **2.4GHz (B+G):** It allows selecting the 802.11b and 802.11g data rates.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
MAC Address 1	**Keep default setting**: WRT-414 will use it's own MAC address to access the wireless LAN. **Press "MAC Clone" button**: It will use PC's MAC address to access the wireless LAN.
Set Security	IF you want to enable security to protect your wireless connection. Please press "Set Security" button and refer to section 6.7 "Security setting for bridge mode" to configure the detail settings.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press "Continue" for configure other settings or "Apply" to restart WRT-414 with new configuration.

6.5 AP Bridge - Point to Multipoint Mode

This function allows WRT-414 to bridge more than 2 wired Ethernet networks together by wireless connection.



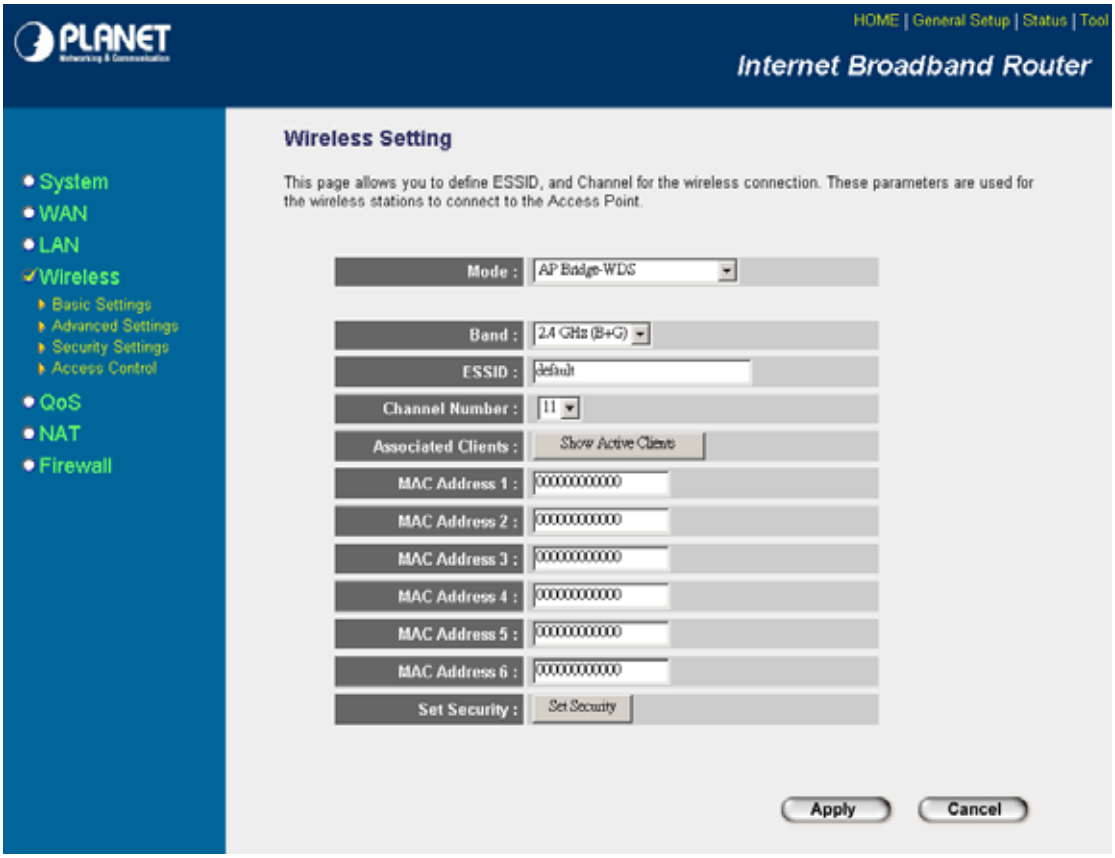
Parameter	Description
Mode	Shows the current operation mode. You may set WRT-414 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It allows to select the transmit rate up to 11Mbps. **2.4GHz (G):** It allows to select the transmit rate up to 54Mbps. **2.4GHz (B+G):** It allows selecting the 802.11b and 802.11g data rates.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
AP MAC Address	If you want to bridge multiple WRT-414 in this mode, you have to enter the MAC addresses of other WRT-414 into the fields.
Set Security	IF you want to enable security to protect your wireless connection. Please press “Set Security” button and refer to section 6.7 “Security setting for bridge mode” to

	configure the detail settings.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

6.6 AP Bridge - WDS Mode

If you want WRT-414 to bridge to other WRT-414 and provide access for other wireless clients at the same time, you have to set the WRT-414 to “AP Bridge - WDS”. Simply speaking, “AP Bridge - WDS” function is the combination of “AP mode” and “AP Bridge-Point to Multi-Point mode”.



Parameter	Description
Mode	Shows the current operation mode. You may set WRT-414 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It allows to select the transmit rate up to 11Mbps. **2.4GHz (G):** It allows to select the transmit rate up to 54Mbps. **2.4GHz (B+G):** It allows selecting the 802.11b and 802.11g data rates.
ESSID	The ESSID (up to 32 printable ASCII characters) is the unique name identified in a

	WLAN. The ID prevents the unintentional merging of two co-located WLANs. Please make sure that the ESSID of all stations in the same WLAN network are the same. The default value is "**default**".
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
Associated Clients	You may press "Show Active Clients" button to check the connected client information. After the button pressed, you will see the dialog box as below:  You may press "Refresh" to get the new client table or "Close" to close this dialog box.
MAC Address 1 ~6	If you want to bridge more than two wired Ethernet networks together with wireless connection, you have to enter the MAC addresses of otherWRT-414s that with join the bridging work into the fields.
Set Security	IF you want to enable security to protect your wireless connection. Please press "Set Security" button and refer to section "3.2.8 Security setting for bridge mode" to configure the detail settings.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press "Continue" for configure other settings or "Apply" to restart WRT-414 with new configuration.

6.7 Security setting of bridge mode

In “AP Bridge-Point to Point mode”, ““AP Bridge-Point to Multi-Point mode” and “AP Bridge-WDS mode”, you can click “Set Security” to add encryption for the communication between the bridged access points. This can protect your wireless network.

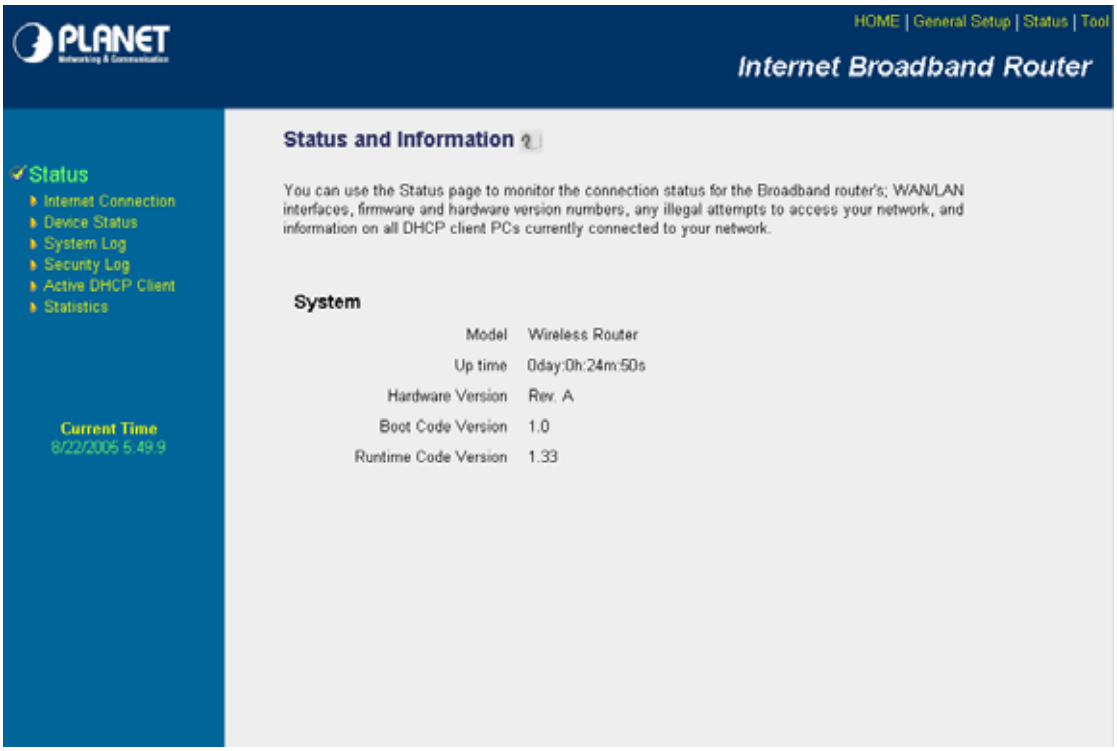
Parameter	Description
Encryption	You can select “None”, “WEP 64bits”, “WEP 128bits”, “WPA (TKIP)” or “WPA2 (AES)” of this option . In default, it is None.
Key Format	This is only used when you select “WEP 64bits” or “WEP 128bits” encryption method. You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the WEP Key. For example: ASCII Characters: guest Hexadecimal Digits: 12345abcde
WEP Key	This is only used when you select “WEP 64bits” or “WEP 128bits” encryption method. The WEP key is used to encrypt data transmitted between the bridged access points. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 10-digit ASCII characters as the encryption keys.
Pre-shared Key	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits

Format	(in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key. For example: Passphrase: iamguest Hex (64 characters): 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted between the bridged access points. Fill the text box by following the rules below. Hex (64 characters): input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

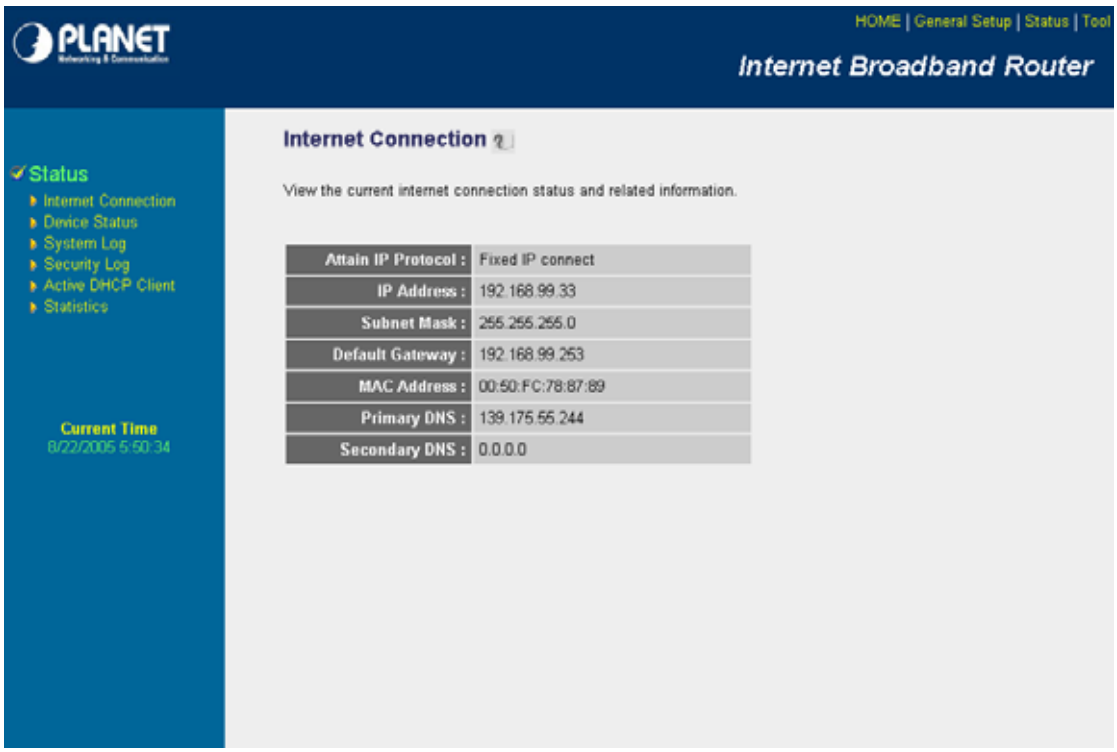
Chapter 7 Status

The Status screen allows you to monitor the current status of your router. You can use the Status page to monitor the connection status of WAN and LAN interfaces, the current firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.



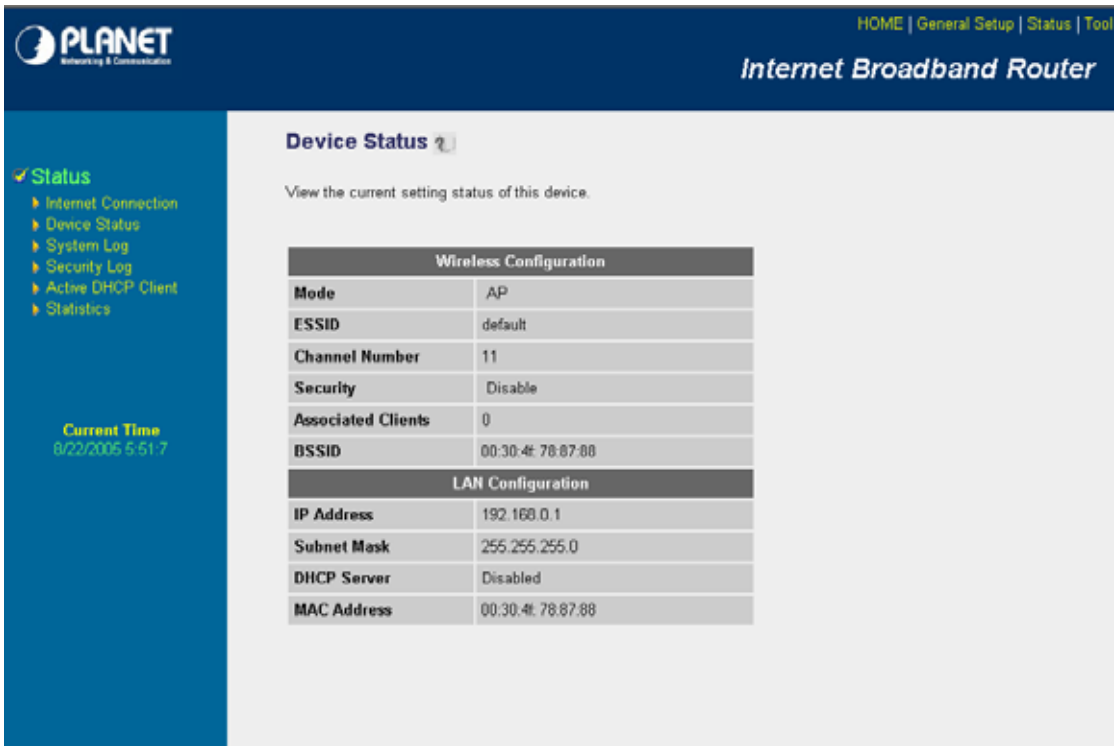
7.1 Internet Connection

View WRT-414's current Internet connection status and other related information.



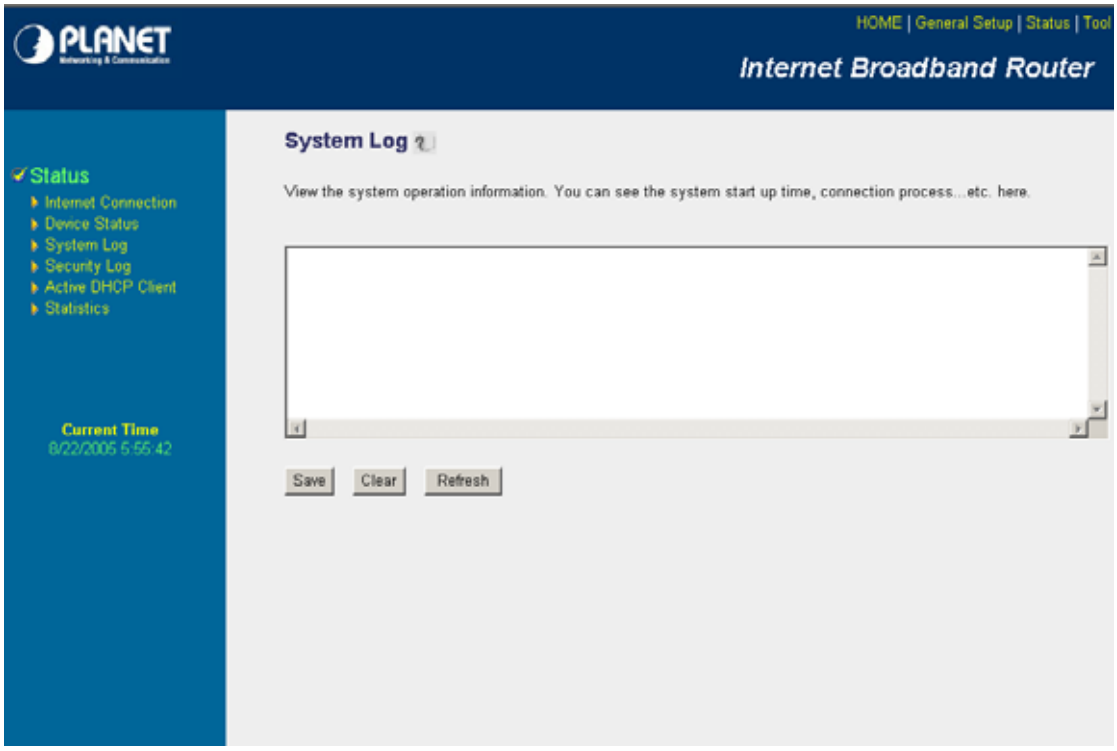
7.2 Device Status

View WRT-414's current configuration settings. The Device Status displays the configuration settings of WLAN and LAN.



7.3 System Log

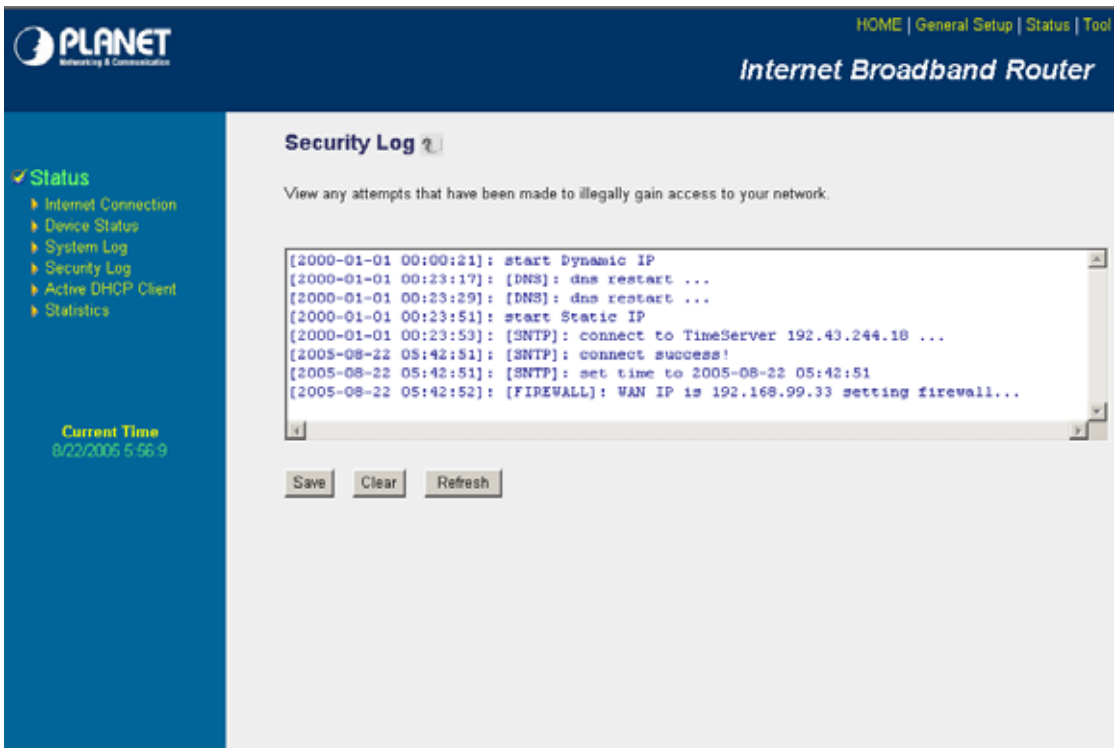
This screen will show you the real-time information of WRT-414.



Parameters	Description
System Log	This page shows the current system log of WRT-414. It displays the working information about WRT-414. About the bottoms of the page, the system log can be saved to a local file by press “Save” button. If there is too much message in this screen, please press “Clear” button to clear the system log . It can be refreshed to get the most updated situation by press “Refresh” button. When the system is powered down, the system log will be cleared.

7.4 Security Log

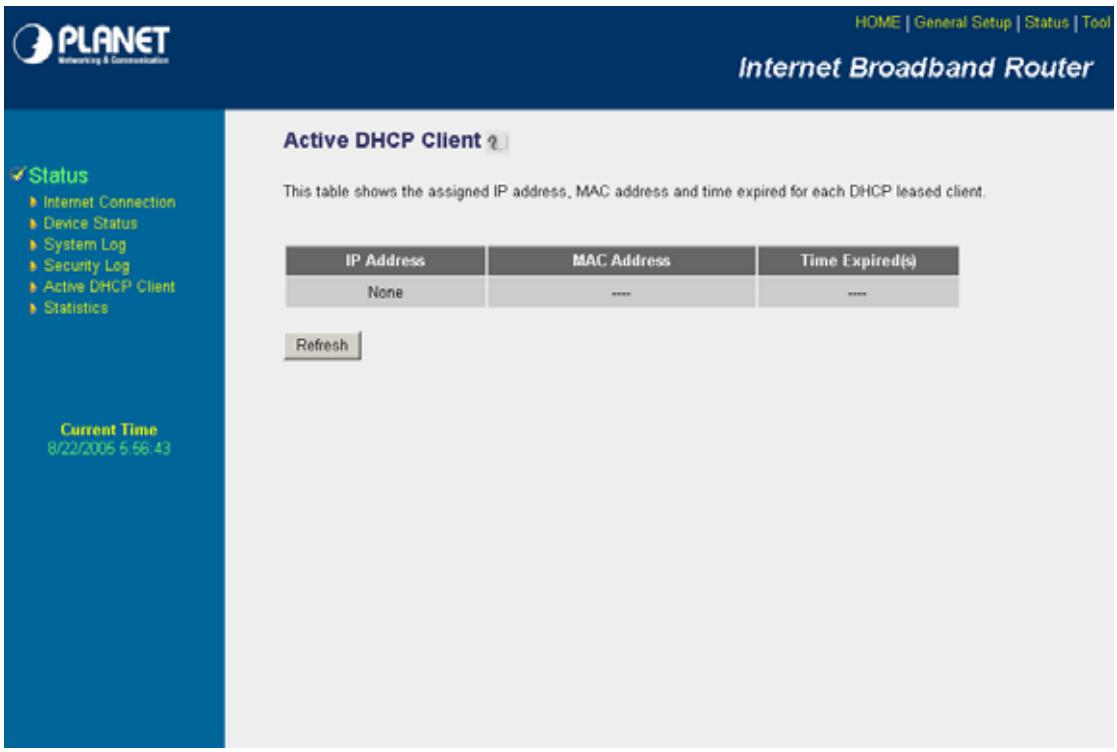
View any attempts that have been made to illegally gain access to your network.



Parameters	Description
Security Log	This page shows the current security log of WRT-414. It displays any illegal attempts to access your network. About the bottoms of the page, the security log can be saved to a local file by press “Save” button. If there is too much message in this screen, please press “Clear” button to clear the system log . It can be refreshed to get the most updated situation by press “Refresh” button. When the system is powered down, the security log will be cleared.

7.5 Active DHCP Client

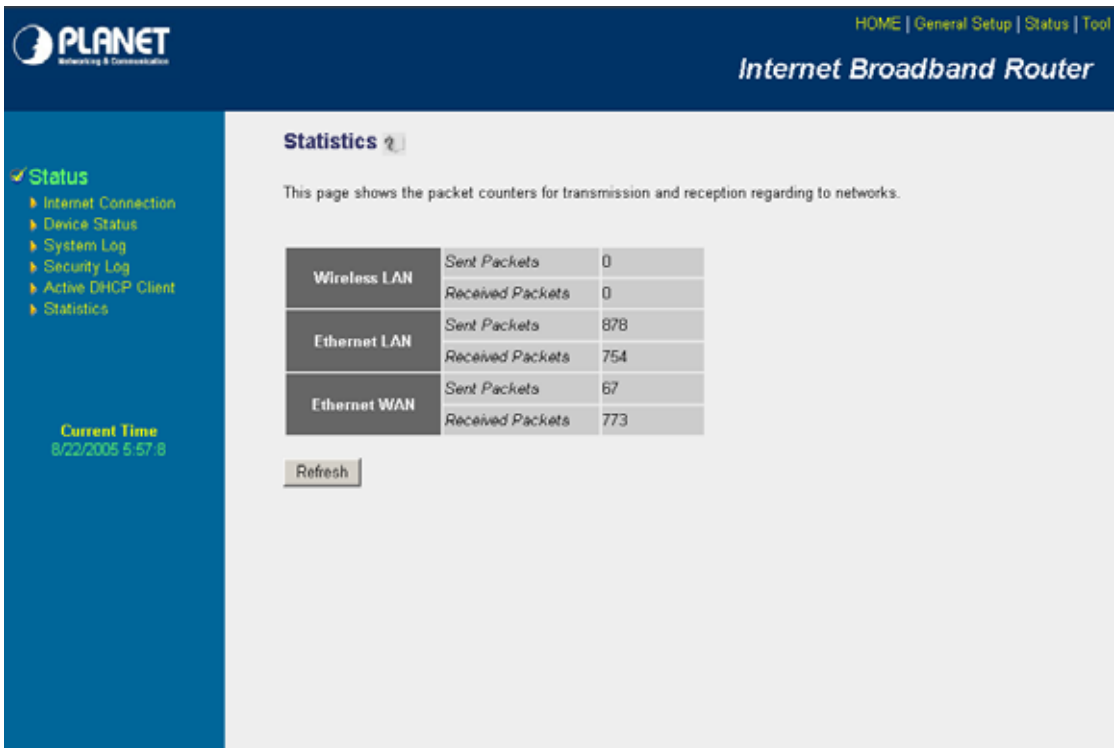
View your client's information that is currently linked to WRT-414's DHCP server.



Parameters	Description
DHCP Client Table	This page shows all the DHCP clients currently connected to your network. The “Active DHCP Client Table” displays the IP address and the MAC address and Time Expired of each Client. Use the Refresh button to get the most updated situation.

7.6 Statistics

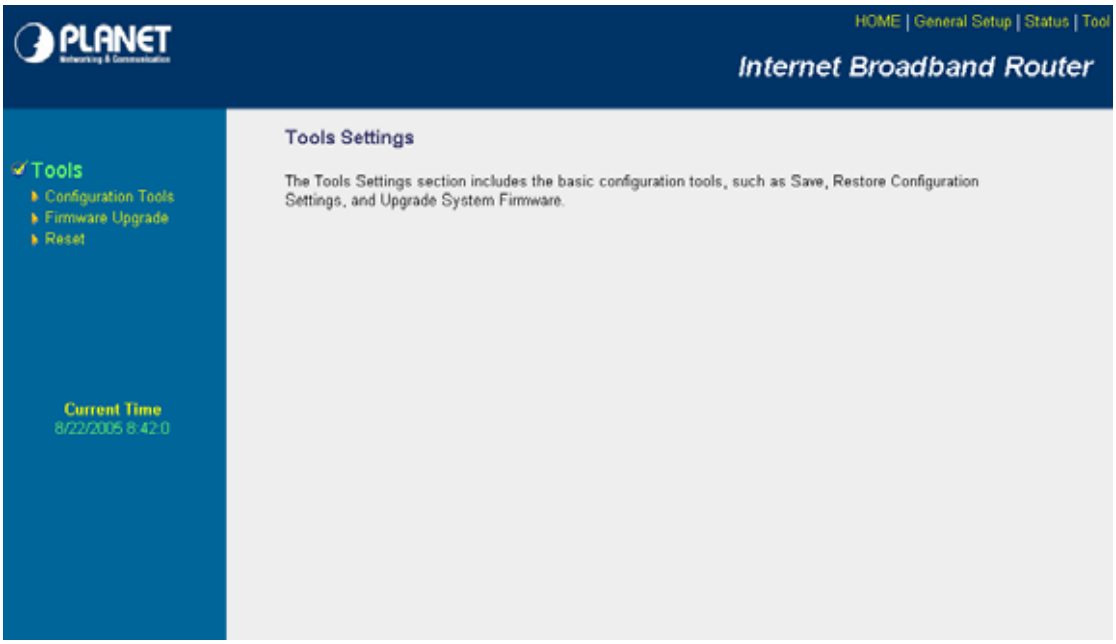
View the statistics of packets sent and received on WLAN, LAN and WAN.



Parameters	Description
Statistics	Shows the counters of packets sent and received on WLAN, LAN and WAN.

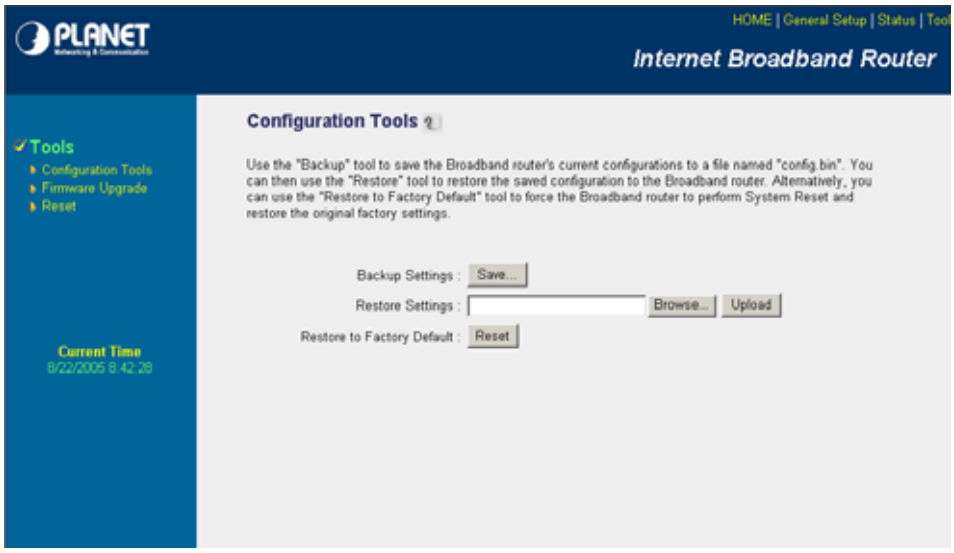
Chapter 8 Tools

This page includes the basic configuration tools, such as Configuration Tools (save or restore configuration settings), Firmware Upgrade (upgrade system firmware) and Reset.



8.1 Configuration Tools

The Configuration Tools screen allows you to “Backup” the router’s current configuration setting. Saving the configuration settings provides an added protection and convenience when problems occur and you have to reset to factory default. With the saved file, you can re-load the saved configuration into the router through the “Restore” function. If extreme problems occur you can use the “Restore to Factory Defaults” selection, this will set all configurations to its original default settings.

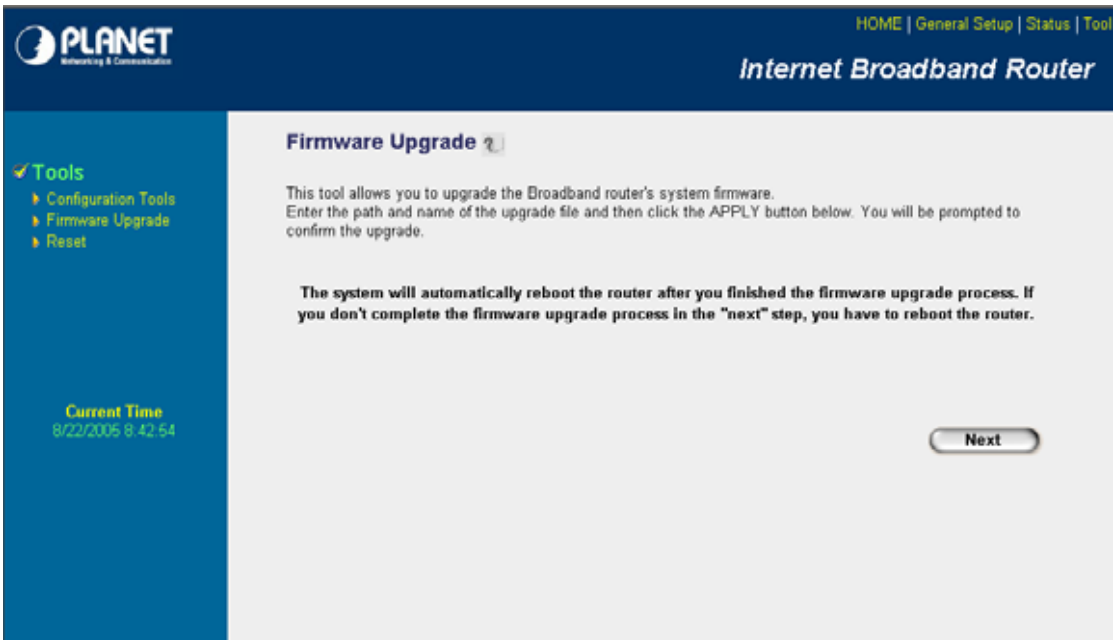


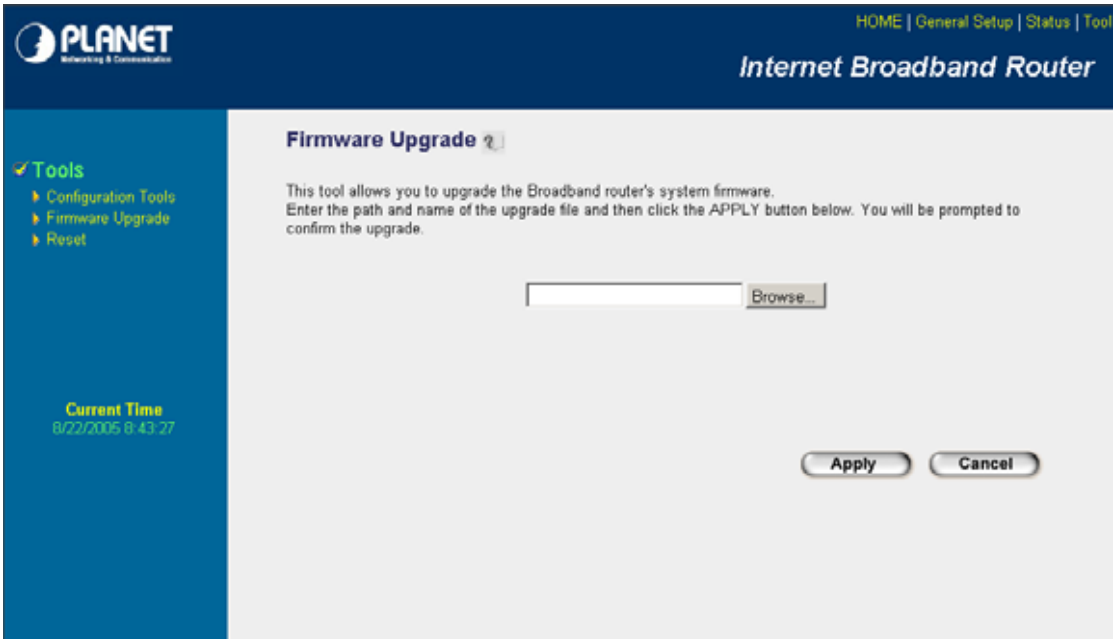
Parameters	Description
Configuration Tools	Use the "**Backup**" tool to save WRT-414 current configuration to a file named "config.bin" in your PC. You can then use the "**Restore**" tool to restore the saved configuration to WRT-414. The "**Restore to Factory Defaults**" tool can force WRT-414 to perform a power reset for restore it to original factory settings.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WRT-414 with new configuration.

8.2 Firmware Upgrade

This page prompt you it allows you to upgrade the router’s firmware. Please press “Next” to continue.





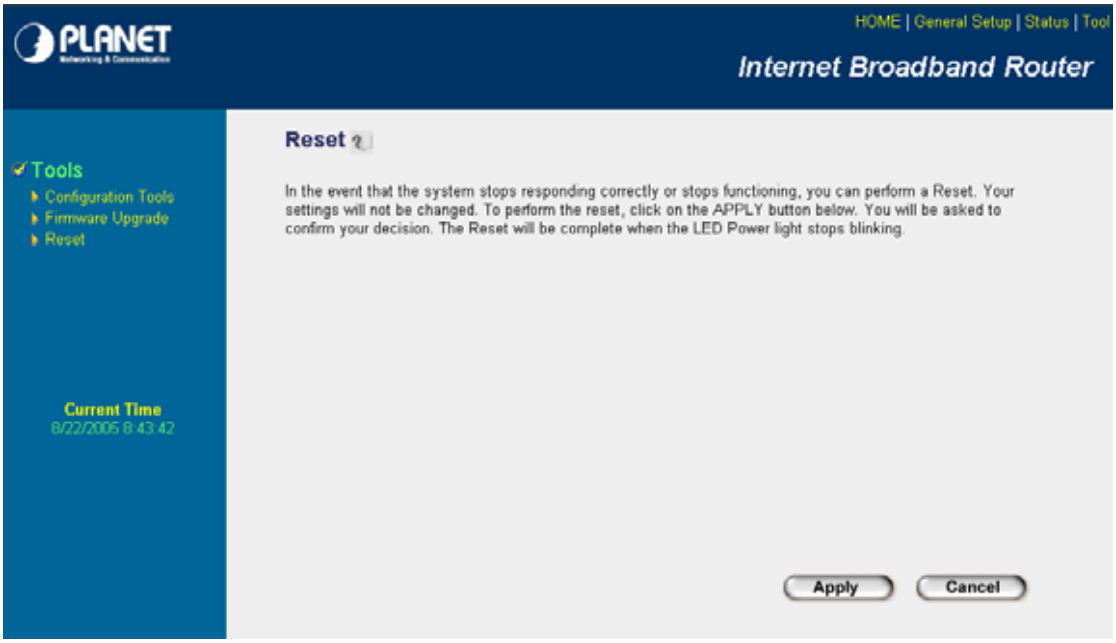
Parameters	Description
Firmware Upgrade	This tool allows you to upgrade WRT-414's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also press the "Browse…" button to find out the firmware file on your PC.

Once you've selected the new firmware file, click "Apply" bottom to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete and WRT-414 restart). After the WRT-414

restart, you can start using the router.

8.3 Reset

You can reset the router's system should any problem exist. The reset function is essentially Re-boot your router.

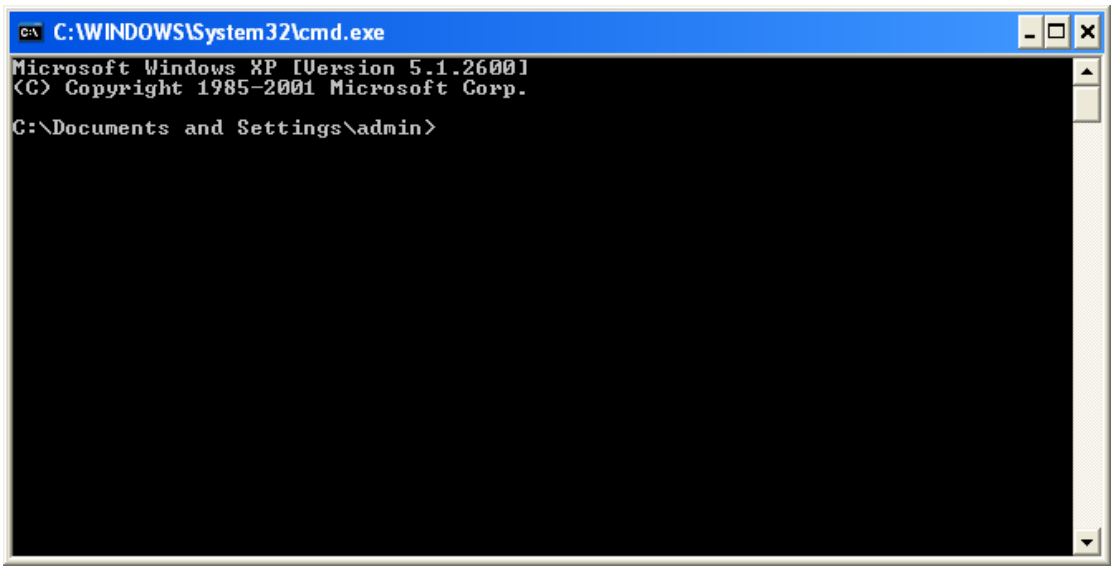


Parameters	Description
Reset	In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. **Your settings will not be changed**. To perform the reset, click on the "Apply" button. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking. Once the reset process is complete you may start using the router again.

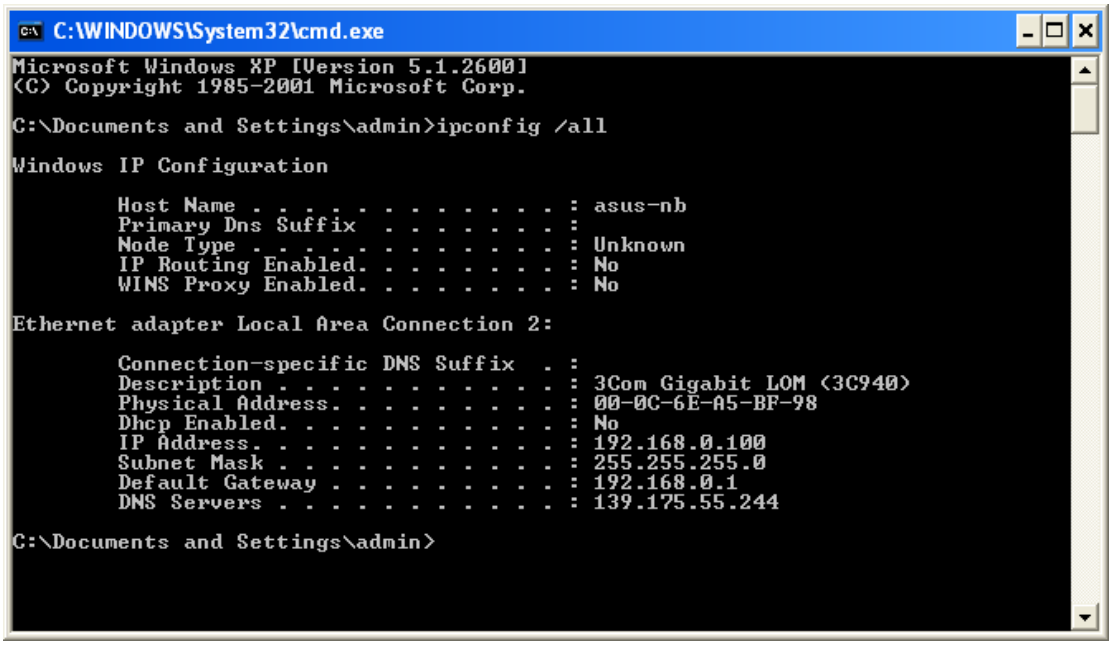
After configuration complete, please click "Apply" button, please wait for a while for the WRT-414 restart.

Appendix A Network Adapter Information

1. In Window's open the Command Prompt program.



2. Type "ipconfig /all" and press "Enter" key.



Then you can see the informations of your network adapter.

Your PC's IP address is the one entitled **IP address** (192.168.0.100).

The router's IP address is the one entitled **Default Gateway** (192.168.0.1).

Your PC's MAC Address is the one entitled **Physical Address** (00-0C-6E-A5-BF-98).

Appendix B Frequently Ask Question

Q. Can I run an application from a remote computer over the wireless network?

A. This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine if it supports operation over a network.

Q. Can I play games with other members of the wireless network?

A. Yes, as long as the game supports multiple plays over a LAN (local area network). Refer to the game's user guide for more information.

Q. What is the IEEE 802.11g standard?

A. The IEEE 802.11g Wireless LAN standards subcommittee, which is formulating a standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

Q. What IEEE 802.11 features are supported?

A. The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

Q. What is Roaming?

A. Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single Wireless Network Access Point. Before using the roaming function, the workstation must make sure that it is the same channel number with the Wireless Network Access Point of dedicated coverage area.

Q. When WRT-414 works with WDS mode, can wireless connect to it?

A. Yes, WDS mode is work as a AP and Bridge at the same time. So the wireless client can access to WDS mode WAP-4033 without problem. When wireless client connect to the remote site via WDS mode, the performance will be 50% then access to the connected WDS mode WAP-4033. Just like connect to AP via a repeater.

Q. How much wired client can connect to Station mode WRT-414?

A. We will suggest you connect max. 5 wired clients to a WRT-414. This more is not suit to connect a

large wired network. If you have much more clients has to connected via wireless, please set WAP-4033 to Bridge mode. Bridge mode will be suit to connect wired LANs together.

Q. Is WRT-414 Bridge mode compatible with other bridge mode device?

A. Yes. WAP-4033 Bridge mode is compatible with WRT-414 and WAP-4033. They are designed with the same chipset. So their bridge mode is compatible to each other.

Appendix C Glossary

Access Point

Access points are way stations in a wireless LAN that are connected to an Ethernet hub or server. Users can roam within the range of access points and their wireless device connections are passed from one access point to the next.

Authentication

Authentication refers to the verification of a transmitted message's integrity.

DMZ

DMZ (DeMilitarized Zone) is a part of an network that is located between a secure LAN and an insecure WAN. DMZ provides a way for some clients to have unrestricted access to the Internet.

Beacon Interval

Refers to the interval between packets sent by access points for the purposes of synchronizing wireless LANs.

DHCP

DHCP (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manually assign permanent IP addresses.

DNS

DNS stands for Domain Name System. DNS converts machine names to the IP addresses that all machines on the net have. It translates from name to address and from address to name.

Domain Name

The domain name typically refers to an Internet site address.

Filter

Filters are schemes which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses.

Firewall

Firewalls are methods used to keep networks secure from malicious intruders and unauthorized access. Firewalls use filters to prevent unwanted packets from being transmitted. Firewalls are typically used to provide secure access to the Internet while keeping an organization's public Web server separate from the internal LAN.

Firmware

Firmware refers to memory chips that retain their content without electrical power (for example, BIOS ROM). The router firmware stores settings made in the interface.

Fragmentation

Refers to the breaking up of data packets during transmission.

FTP

FTP (File Transfer Protocol) is used to transfer files over a TCP/IP network, and is typically used for

transferring large files or uploading the HTML pages for a Web site to the Web server.

Gateway

Gateways are computers that convert protocols enabling different networks, applications, and operating systems to exchange information.

Host Name

The name given to a computer or client station that acts as a source for information on the network.

HTTP

HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTP establishes a connection with a Web server and transmits HTML pages to client browser (for example Windows IE). HTTP addresses all begin with the prefix 'http://' prefix (for example, *http://www.yahoo.com*).

ICMP

ICMP (Internet Control Message Protocol) is a TCP/IP protocol used to send error and control messages over the LAN (for example, it is used by the router to notify a message sender that the destination node is not available).

IP

IP (Internet Protocol) is the protocol in the TCP/IP communications protocol suite that contains a network address and allows messages to be routed to a different network or subnet. However, IP does not ensure delivery of a complete message—TCP provides the function of ensuring delivery.

IP Address

The IP (Internet Protocol) address refers to the address of a computer attached to a TCP/IP network. Every client and server station must have a unique IP address. Clients are assigned either a permanent address or have one dynamically assigned to them via DHCP. IP addresses are written as four sets of numbers separated by periods (for example, 211.23.181.189).

ISP

An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines.

LAN

LANs (Local Area Networks) are networks that serve users within specific geographical areas, such as in a company building. LANs are comprised of servers, workstations, a network operating system, and communications links such as the router.

MAC Address

A MAC address is a unique serial number burned into hardware adapters, giving the adapter a unique identification.

Metric

A number that indicates how long a packet takes to get to its destination.

MTU

MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network.

Messages larger than the MTU are divided into smaller packets.

NAT

NAT (Network Address Translation - also known as IP masquerading) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa). NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN.

(Network) Administrator

The network administrator is the person who manages the LAN within an organization. The administrator's job includes ensuring network security, keeping software, hardware, and firmware up-to-date, and keeping track of network activity.

NTP

NTP (Network Time Protocol) is used to synchronize the real-time clock in a computer. Internet primary and secondary servers synchronize to Coordinated Universal Time (UTC).

Packet

A packet is a portion of data that is transmitted in network communications. Packets are also sometimes called frames and datagrams. Packets contain not only data, but also the destination IP address.

Ping

Ping (Packet Internet Groper) is a utility used to find out if a particular IP address is present online, and is usually used by networks for debugging.

Port

Ports are the communications pathways in and out of computers and network devices (routers and switches). Most PCs have serial and parallel ports, which are external sockets for connecting devices such as printers, modems, and mice. All network adapters use ports to connect to the LAN. Ports are typically numbered.

PPPoE

PPPoE (Point-to-Point Protocol Over Ethernet) is used for running PPP protocol (normally used for dial-up Internet connections) over an Ethernet.

Preamble

Preamble refers to the length of a CRC (Cyclic Redundancy Check) block that monitors communications between roaming wireless enabled devices and access points.

Protocol

A protocol is a rule that governs the communication of data.

RIP

RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination.

RTS

RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data.

Server

Servers are typically powerful and fast machines that store programs and data. The programs and data are shared by client machines (workstations) on the network.

SMTP

SMTP (Simple Mail Transfer Protocol) is the standard Internet e-mail protocol. SMTP is a TCP/IP protocol defining message format and includes a message transfer agent that stores and forwards mail.

SNMP

SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol. SNMP hardware or software components transmit network device activity data to the workstation used to oversee the network.

SSID

SSID (Service Set Identifier) is a security measure used in WLANs. The SSID is a unique identifier attached to packets sent over WLANs. This identifier emulates a password when a wireless device attempts communication on the WLAN. Because an SSID distinguishes WLANS from each other, access points and wireless devices trying to connect to a WLAN must use the same SSID.

Subnet Mask

Subnet Masks are used by IP protocol to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an incoming IP address to determine whether to accept or reject the packet.

SysLog Server

A SysLog server monitors incoming Syslog messages and decodes the messages for logging purposes.

TCP

(Transmission Control Protocol) is the transport protocol in TCP/IP that ensures messages over the network are transmitted accurately and completely.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in realtime video and audio transmission).

The IP component of TCP/IP provides data routability, meaning that data packets contain the destination station and network addresses, enabling TCP/IP messages to be sent to multiple networks within the LAN or in the WAN.

Telnet

Telnet is a terminal emulation protocol commonly used on the Internet and TCP- or IP-based networks. Telnet is used for connecting to remote devices and running programs. Telnet is an integral component of the TCP/IP communications protocol.

UDP

(User Datagram Protocol) is a protocol within TCP/IP that is used to transport information when accurate

delivery isn't necessary (for example, real-time video and audio where packets can be dumped as there is no time for retransmitting the data).

Virtual Servers

Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).

WEP

WEP (Wired Equivalent Privacy) is the de facto security protocol for wireless LANs, providing the "equivalent" security available in hardwired networks.

Wireless LAN

Wireless LANs (WLANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.

WLAN

WLANs (Wireless LANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.

WAN

WAN (Wide Area Network) is a communications network that covers a wide geographic area such as a country (contrasted with a LAN, which covers a small area such as a company building).